

(51) Int. Cl. ⁷

GO6F 12/14
GO6F 17/60
HO4L 9/08
HO4N 7/173

F I

GO6F 12/14 310K
GO6F 17/60 142
GO6F 17/60 302E
GO6F 17/60 318G
GO6F 17/60 512

テーマコード (参考)

5B017
5C064
5J104

審査請求 未請求 請求項の数 16 O L (全 44 頁) 最終頁に続く

(21) 出願番号 特願2002-213700 (P2002-213700)
(22) 出願日 平成14年7月23日 (2002. 7. 23)

(71) 出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
(74) 代理人 100093241
弁理士 宮田 正昭
(74) 代理人 100101801
弁理士 山田 英治
(74) 代理人 100086531
弁理士 澤田 俊夫
(72) 発明者 北谷 義道
東京都品川区北品川6丁目7番35号 ソ
ニー株式会社内
(72) 発明者 栗屋 志伸
東京都品川区北品川6丁目7番35号 ソ
ニー株式会社内

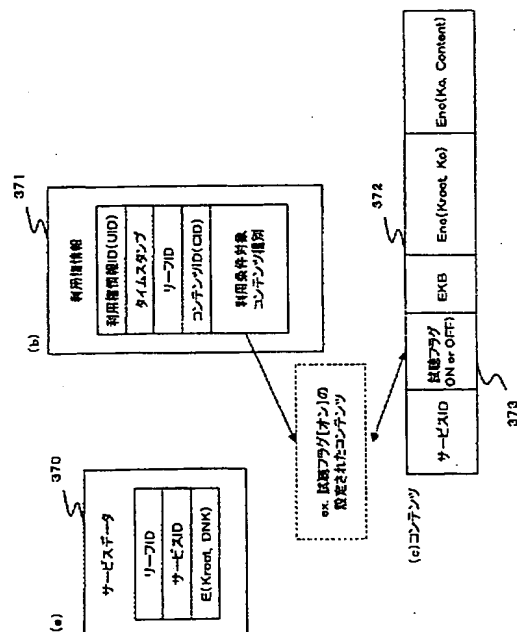
最終頁に続く

(54) 【発明の名称】 情報処理装置、および情報処理方法、並びにコンピュータ・プログラム

(57) 【要約】

【課題】 コンテンツの利用権情報に基づくコンテンツ利用構成において、コンテンツ試聴における改良された処理を実現する装置、方法を提供する。

【解決手段】 クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報 (Default Usage Right) を取得し、コンテンツの購入処理を伴わない試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生の可否を判定する。試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。



1

【特許請求の範囲】

【請求項 1】

暗号化コンテンツの復号および再生処理を実行する情報処理装置であり、
コンテンツ再生条件として、コンテンツ利用権情報を参照し、該コンテンツ利用権情報に基づく再生処理を実行する制御手段を有し、
前記制御手段は、
購入コンテンツの再生に際しては、コンテンツ対応の利用権情報の記述に基づく再生可否判定を実行し、
コンテンツの試聴処理に際しては、試聴処理に対応したコンテンツ利用権情報としてのデフォルト利用権情報の記述に基づく再生可否判定を実行する構成を有することを特徴とする情報処理装置。

【請求項 2】

前記デフォルト利用権情報は、コンテンツファイルに設定された試聴フラグの設定値に基づくコンテンツ再生権許可情報を有し、
前記制御手段は、
コンテンツの試聴処理に際しては、試聴対象コンテンツに付加された試聴フラグを検証し、該検証結果に基づいて、再生の可否を判定する構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記情報処理装置は、
コンテンツの購入再生処理に適用する購入再生実行アプリケーションと、コンテンツの試聴処理に適用する試聴処理実行アプリケーションを格納し、
前記制御手段は、
外部から入力する起動ファイルに基づいて、前記購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択して実行する構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】

前記情報処理装置は、
コンテンツの購入再生処理に適用する購入再生実行アプリケーションと、コンテンツの試聴処理に適用する試聴処理実行アプリケーションを格納し、
前記制御手段は、
外部から入力する起動ファイルに設定された拡張子に基づいて、前記購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択して実行する構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】

前記暗号化コンテンツは、
コンテンツキー Kc により暗号化されたコンテンツであり、前記コンテンツキー Kc は、有効化キープブロック (EKB) 配信ツリー構成を適用して提供される有効化キープブロック (EKB) の復号により取得可能なキーの

2

適用によってのみ取得可能なキーであり、

前記制御手段は、

前記有効化キープブロック (EKB) の復号処理によるコンテンツキー取得処理を実行する構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】

コンテンツ再生を実行するクライアントに対するコンテンツ利用権情報を発行するライセンスサーバとしての情報処理装置であり、

10 クライアントからの登録要求に応じて、暗号化コンテンツの復号処理の際に必要なデバイスノードキー (DNK) を含む有効化キープブロック (EKB) を格納したサービスデータと、

クライアントにおけるコンテンツの試聴処理において再生可否判定に適用するコンテンツ利用権情報としてのデフォルト利用権情報とを生成し、クライアントに対して発行する処理を実行する構成を有することを特徴とする情報処理装置。

【請求項 7】

20 前記情報処理装置は、
コンテンツファイルに設定された試聴フラグの設定値に基づくコンテンツ再生権許可情報を格納したデフォルト利用権情報を生成する処理を実行する構成を有することを特徴とする請求項 6 に記載の情報処理装置。

【請求項 8】

暗号化コンテンツの復号および再生処理を実行する情報処理方法であり、

コンテンツ再生条件として、コンテンツ利用権情報を参照し、該コンテンツ利用権情報に基づく再生処理を実行するコンテンツ再生制御ステップを有し、

30 前記コンテンツ再生制御ステップは、さらに、
購入コンテンツの再生処理であるかコンテンツの試聴処理であるかを判定するステップと、

購入コンテンツの再生処理であることを条件として実行するコンテンツ対応の利用権情報の記述に基づく再生可否判定処理ステップと、

40 コンテンツの試聴処理であることを条件として実行する試聴処理に対応したコンテンツ利用権情報としてのデフォルト利用権情報の記述に基づく再生可否判定処理ステップとを含むことを特徴とする情報処理方法。

【請求項 9】

前記デフォルト利用権情報は、コンテンツファイルに設定された試聴フラグの設定値に基づくコンテンツ再生権許可情報を有し、

前記コンテンツ再生制御ステップは、

コンテンツの試聴処理に際しては、試聴対象コンテンツに付加された試聴フラグを検証し、該検証結果に基づいて、再生の可否を判定することを特徴とする請求項 8 に記載の情報処理方法。

50 【請求項 10】

前記情報処理方法は、さらに、外部から入力する起動ファイルに基づいて、購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択する選択ステップを有し、前記コンテンツ再生制御ステップは、前記選択ステップにおいて選択したアプリケーションに従って実行することを特徴とする請求項8に記載の情報処理方法。

【請求項11】

前記情報処理方法は、さらに、外部から入力する起動ファイルの拡張子を判別するステップと、判別した起動ファイルの拡張子に基づいて、購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択する選択ステップを有し、前記コンテンツ再生制御ステップは、前記選択ステップにおいて選択したアプリケーションに従って実行することを特徴とする請求項8に記載の情報処理方法。

【請求項12】

前記暗号化コンテンツは、コンテンツキーKcにより暗号化されたコンテンツであり、前記コンテンツキーKcは、有効化キーブロック(EKB)配信ツリー構成を適用して提供される有効化キーブロック(EKB)の復号により取得可能なキーの適用によってのみ取得可能なキーであり、前記コンテンツ再生制御ステップは、前記有効化キーブロック(EKB)の復号処理によるコンテンツキー取得処理を実行するステップを含むことを特徴とする請求項8に記載の情報処理方法。

【請求項13】

コンテンツ再生を実行するクライアントに対するコンテンツ利用権情報を発行するライセンスサーバにおける情報処理方法であり、クライアントからの登録要求を受信するステップと、前記登録要求の受信に応じて、暗号化コンテンツの復号処理の際に必要となるデバイスノードキー(DNK)を含む有効化キーブロック(EKB)を格納したサービスデータと、クライアントにおけるコンテンツの試聴処理において再生可否判定に適用するコンテンツ利用権情報としてのデフォルト利用権情報とを生成するステップと、生成したサービスデータとデフォルト利用権情報とをクライアントに対して送信するステップと、を有することを特徴とする情報処理方法。

【請求項14】

前記情報処理方法において、デフォルト利用権情報を、コンテンツファイルに設定された試聴フラグの設定値に基づくコンテンツ再生権許可情報を格納した利用権情報として生成する処理を実行す

ることを特徴とする請求項13に記載の情報処理方法。

【請求項15】

暗号化コンテンツの復号および再生処理実行プログラムを記述したコンピュータ・プログラムであって、購入コンテンツの再生処理であるかコンテンツの試聴処理であるかを判定するステップと、購入コンテンツの再生処理であることを条件として実行するコンテンツ対応の利用権情報の記述に基づく再生可否判定処理ステップと、コンテンツの試聴処理であることを条件として実行する試聴処理に対応したコンテンツ利用権情報としてのデフォルト利用権情報の記述に基づく再生可否判定処理ステップと、を有することを特徴とするコンピュータ・プログラム。

【請求項16】

コンテンツ再生を実行するクライアントに対するコンテンツ利用権情報を発行するライセンスサーバにおける情報処理実行プログラムを記述したコンピュータ・プログラムであって、クライアントからの登録要求を受信するステップと、前記登録要求の受信に応じて、暗号化コンテンツの復号処理の際に必要となるデバイスノードキー(DNK)を含む有効化キーブロック(EKB)を格納したサービスデータと、クライアントにおけるコンテンツの試聴処理において再生可否判定に適用するコンテンツ利用権情報としてのデフォルト利用権情報とを生成するステップと、生成したサービスデータとデフォルト利用権情報とをクライアントに対して送信するステップと、を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。特に、コンテンツの再生等の利用時におけるコンテンツ利用権の確認を実現し、また、コンテンツの試聴、試写処理を可能としてユーザに対するフレキシブルなコンテンツ利用態様を実現した情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。

【0002】

【従来の技術】

昨今、音楽データ、ゲームプログラム、画像データ等、様々なソフトウェアデータ(以下、これらをコンテンツ(Content)と呼ぶ)の、インターネット等のネットワーク、あるいは、メモリカード、HD、DVD、CD等の流通可能な記憶媒体を介した流通が盛んになっている。これらの流通コンテンツは、ユーザの所有するPC(Personal Computer)、記録再生器、再生専用器、あるいはゲーム機器内の記憶手段、

例えばHD、フラッシュメモリを有するカード型記憶装置、CD、DVD等に格納され、再生処理が実行される。

【0003】

記録再生装置、ゲーム機器、PC等の情報機器には、コンテンツをネットワークから受信するためのインタフェース、あるいはメモリカード、HD、DVD、CD等にアクセスするためのインタフェースを有し、コンテンツの再生に必要な制御手段、プログラム、データのメモリ領域として使用されるRAM、ROM等を有する。

【0004】

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用される記録再生装置、ゲーム機器、PC等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により、例えば内蔵、あるいは着脱自在の記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【0005】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【0006】

また、コンテンツと、コンテンツを利用する利用権とを独立に管理し、ユーザに提供する構成が提案されている。この構成において、ユーザは、例えば暗号化されたコンテンツを取得し、さらに、利用権データを購入することにより、利用権データから取得可能な鍵データ等に基づいて、暗号化コンテンツの復号用の鍵（コンテンツ鍵）を取得して、コンテンツを利用する。

【0007】

利用権データには、ユーザのコンテンツ利用許可態様の設定情報が格納され、その許可情報において許された範囲でのコンテンツの利用が可能となるといったシステムが提案されている。

【0008】

【発明が解決しようとする課題】

このように、コンテンツとコンテンツ利用権とを独立に管理し、ユーザに提供するシステムにおいては、コンテンツの利用、例えば音楽データ、画像データの再生、または配信、あるいはダウンロード処理に際して、利用権データのチェックが実行される。

【0009】

このような構成において、利用権チェックの際、ユーザがコンテンツの利用をする権利がないと判定された場合

には、コンテンツの再生、配信、ダウンロードが実行されないことになる。

【0010】

しかしながら、コンテンツの購入以前に、コンテンツの一部等を試聴、あるいは試写を行なって、コンテンツの内容を確認した上で、コンテンツの購入を行ないたいという要望があるのも事実であり、このような場合に、通常のコンテンツ利用権のチェック処理を行なえば、利用権が無いとの判定によって、コンテンツ再生等の処理が拒否されてしまうことになる。

【0011】

このような状況に対応するためには、利用権を全く考慮しないフリーのサンプルデータをユーザに対して配布する構成とすることも可能であるが、ほとんどのコンテンツには著作権者の著作権、頒布者の頒布権が存在する。従って、コンテンツの一部であっても、コンテンツが無秩序に流通し、ユーザ間で無断でコピーが行われるといった事態は好ましいことではない。

【0012】

本発明は、このような状況に鑑みてなされたものであり、ユーザがコンテンツの正規な購入処理を行なって利用権に基づいた正当なコンテンツ利用を可能とするとともに、コンテンツを購入を伴わないコンテンツ試聴、あるいは試写を行なうことを可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

【0013】

本発明は、さらに、試聴データ、試写データの無秩序な二次流通の防止を可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

【0014】

【課題を解決するための手段】

本発明の第1の側面は、暗号化コンテンツの復号および再生処理を実行する情報処理装置であり、コンテンツ再生条件として、コンテンツ利用権情報を参照し、該コンテンツ利用権情報に基づく再生処理を実行する制御手段を有し、

前記制御手段は、購入コンテンツの再生に際しては、コンテンツ対応の利用権情報の記述に基づく再生可否判定を実行し、コンテンツの試聴処理に際しては、試聴処理に対応したコンテンツ利用権情報としてのデフォルト利用権情報の記述に基づく再生可否判定を実行する構成を有することを特徴とする情報処理装置にある。

【0015】

さらに、本発明の情報処理装置の一実施態様において、前記デフォルト利用権情報は、コンテンツファイルに設定された試聴フラグの設定値に基づくコンテンツ再生権

許可情報を有し、前記制御手段は、コンテンツの試聴処理に際しては、試聴対象コンテンツに付加された試聴フラグを検証し、該検証結果に基づいて、再生の可否を判定する構成であることを特徴とする。

【0016】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツの購入再生処理に適用する購入再生実行アプリケーションと、コンテンツの試聴処理に適用する試聴処理実行アプリケーションを格納し、前記制御手段は、外部から入力する起動ファイルに基づいて、前記購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択して実行する構成であることを特徴とする。

【0017】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツの購入再生処理に適用する購入再生実行アプリケーションと、コンテンツの試聴処理に適用する試聴処理実行アプリケーションを格納し、前記制御手段は、外部から入力する起動ファイルに設定された拡張子に基づいて、前記購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択して実行する構成であることを特徴とする。

【0018】

さらに、本発明の情報処理装置の一実施態様において、前記暗号化コンテンツは、コンテンツキーKcにより暗号化されたコンテンツであり、前記コンテンツキーKcは、有効化キーブロック(EKB)配信ツリー構成を適用して提供される有効化キーブロック(EKB)の復号により取得可能なキーの適用によってのみ取得可能なキーであり、前記制御手段は、前記有効化キーブロック(EKB)の復号処理によるコンテンツキー取得処理を実行する構成であることを特徴とする。

【0019】

さらに、本発明の第2の側面は、コンテンツ再生を実行するクライアントに対するコンテンツ利用権情報を発行するライセンスサーバとしての情報処理装置であり、クライアントからの登録要求に応じて、暗号化コンテンツの復号処理の際に必要なデバイスノードキー(DNK)を含む有効化キーブロック(EKB)を格納したサービスデータと、クライアントにおけるコンテンツの試聴処理において再生可否判定に適用するコンテンツ利用権情報としてのデフォルト利用権情報とを生成し、クライアントに対して発行する処理を実行する構成を有することを特徴とする情報処理装置にある。

【0020】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、コンテンツファイルに設定された

試聴フラグの設定値に基づくコンテンツ再生権許可情報を格納したデフォルト利用権情報を生成する処理を実行する構成を有することを特徴とする。

【0021】

さらに、本発明の第3の側面は、暗号化コンテンツの復号および再生処理を実行する情報処理方法であり、コンテンツ再生条件として、コンテンツ利用権情報を参照し、該コンテンツ利用権情報に基づく再生処理を実行するコンテンツ再生制御ステップを有し、前記コンテンツ再生制御ステップは、さらに、購入コンテンツの再生処理であるかコンテンツの試聴処理であるかを判定するステップと、購入コンテンツの再生処理であることを条件として実行するコンテンツ対応の利用権情報の記述に基づく再生可否判定処理ステップと、コンテンツの試聴処理であることを条件として実行する試聴処理に対応したコンテンツ利用権情報としてのデフォルト利用権情報の記述に基づく再生可否判定処理ステップとを含むことを特徴とする情報処理方法にある。

【0022】

さらに、本発明の情報処理方法の一実施態様において、前記デフォルト利用権情報は、コンテンツファイルに設定された試聴フラグの設定値に基づくコンテンツ再生権許可情報を有し、前記コンテンツ再生制御ステップは、コンテンツの試聴処理に際しては、試聴対象コンテンツに付加された試聴フラグを検証し、該検証結果に基づいて、再生の可否を判定することを特徴とする。

【0023】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、外部から入力する起動ファイルに基づいて、購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択する選択ステップを有し、前記コンテンツ再生制御ステップは、前記選択ステップにおいて選択したアプリケーションに従って実行することを特徴とする。

【0024】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、外部から入力する起動ファイルの拡張子を判別するステップと、判別した起動ファイルの拡張子に基づいて、購入再生実行アプリケーション、または試聴処理実行アプリケーションのいずれかを選択する選択ステップを有し、前記コンテンツ再生制御ステップは、前記選択ステップにおいて選択したアプリケーションに従って実行することを特徴とする。

【0025】

さらに、本発明の情報処理方法の一実施態様において、前記暗号化コンテンツは、コンテンツキーKcにより暗号化されたコンテンツであり、前記コンテンツキーKcは、有効化キーブロック(EKB)配信ツリー構成を適

9

用して提供される有効化キーブロック（EKB）の復号により取得可能なキーの適用によってのみ取得可能なキーであり、前記コンテンツ再生制御ステップは、前記有効化キーブロック（EKB）の復号処理によるコンテンツキー取得処理を実行するステップを含むことを特徴とする。

【0026】

さらに、本発明の第4の側面は、コンテンツ再生を実行するクライアントに対するコンテンツ利用権情報を発行するライセンスサーバにおける情報処理方法であり、クライアントからの登録要求を受信するステップと、前記登録要求の受信に応じて、暗号化コンテンツの復号処理の際に必要なデバイスノードキー（DNK）を含む有効化キーブロック（EKB）を格納したサービスデータと、クライアントにおけるコンテンツの試聴処理において再生可否判定に適用するコンテンツ利用権情報としてのデフォルト利用権情報とを生成するステップと、生成したサービスデータとデフォルト利用権情報とをクライアントに対して送信するステップと、を有することを特徴とする情報処理方法にある。

【0027】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法において、デフォルト利用権情報を、コンテンツファイルに設定された試聴フラグの設定値に基づくコンテンツ再生権許可情報を格納した利用権情報として生成する処理を実行することを特徴とする。

【0028】

さらに、本発明の第5の側面は、暗号化コンテンツの復号および再生処理実行プログラムを記述したコンピュータ・プログラムであって、購入コンテンツの再生処理であるかコンテンツの試聴処理であるかを判定するステップと、購入コンテンツの再生処理であることを条件として実行するコンテンツ対応の利用権情報の記述に基づく再生可否判定処理ステップと、コンテンツの試聴処理であることを条件として実行する試聴処理に対応したコンテンツ利用権情報としてのデフォルト利用権情報の記述に基づく再生可否判定処理ステップと、を有することを特徴とするコンピュータ・プログラムにある。

【0029】

さらに、本発明の第6の側面は、コンテンツ再生を実行するクライアントに対するコンテンツ利用権情報を発行するライセンスサーバにおける情報処理実行プログラムを記述したコンピュータ・プログラムであって、クライアントからの登録要求を受信するステップと、

10

前記登録要求の受信に応じて、暗号化コンテンツの復号処理の際に必要なデバイスノードキー（DNK）を含む有効化キーブロック（EKB）を格納したサービスデータと、クライアントにおけるコンテンツの試聴処理において再生可否判定に適用するコンテンツ利用権情報としてのデフォルト利用権情報とを生成するステップと、生成したサービスデータとデフォルト利用権情報とをクライアントに対して送信するステップと、を有することを特徴とするコンピュータ・プログラムにある。

【0030】

【作用】

本発明の構成によれば、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報（Default Usage Right）を取得し、コンテンツの購入処理を伴わない試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生が許可され、ユーザは、コンテンツの購入を実行することなく、コンテンツの試聴再生が可能となる。また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまふことが防止される。

【0031】

さらに、本発明の構成によれば、コンテンツの購入処理を伴わない試聴処理においても、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB〔EKB（H）〕と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB〔EKB（S）〕に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴処理においても再生権限を限定した範囲として設定可能となる。

【0032】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0033】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構

成の装置が同一筐体内にあるものには限らない。

【0034】

【発明の実施の形態】

以下、本発明の構成について詳細に説明する。なお、説明は、以下に示す各項目に従って行なう。

1. コンテンツ提供システム概要
2. キー配信構成としてのツリー（木）構造について
3. EKBを使用したキーの配布
4. EKBのフォーマット
5. ツリーのカテゴリ分類
6. コンテンツ購入および試聴処理
7. バックアップ／リストア処理
8. リコメンドファイルによるコンテンツの二次配信

【0035】

【1. コンテンツ提供システム概要】

図1は、本発明を適用したコンテンツ提供システムの概要を説明する図である。コンテンツの利用を行なうクライアント10は、コンテンツを利用、すなわち再生可能な機器としての情報処理装置である。例えばPC、PDA等、各種の情報処理装置が含まれる。クライアント10は、ソフトウェアとしてブラウザ11、クライアントアプリケーション12を有し、CPU等の制御手段によりブラウザ11、クライアントアプリケーション12他のプログラムが実行される。

【0036】

クライアントアプリケーション12は、クライアントにおけるコンテンツの購入および試聴処理、後段において説明するサービスデータ、コンテンツ利用権情報を含むライセンス情報の取得処理、コンテンツおよびライセンス情報のバックアップ／リストア処理、コンテンツ利用権の確認処理、コンテンツ再生管理処理、あるいは、二次配信用のコンテンツファイルとしてのリコメンドファイルの生成処理等を実行するアプリケーションであり、以下、詳細に説明する処理プログラムとして、クライアントの情報処理装置に格納される。なお、本明細書においては、「試聴」は、音声データの試聴のみならず、画像データの試写を包含する意味として用いる。

【0037】

クライアント10は、例えばインターネット等の通信網を介してショップサーバ21、ライセンスサーバ22、およびコンテンツサーバ23と接続される。コンテンツサーバ23は、クライアント10に対してコンテンツを提供する。ライセンスサーバ22は、クライアントが利用するコンテンツの利用権情報をクライアント10に対して提供する。また、ショップサーバ21は、クライアント10がコンテンツを購入する際の窓口として機能し、購入または試聴可能コンテンツをブラウザを介して提示し、クライアントからの購入あるいは試聴の要求を受け付ける。また、必要に応じて購入コンテンツに関する課金処理を行なう。

【0038】

さらに、ショップサーバ21、およびライセンスサーバ22には、管理システム31が接続される。管理システム31は、ショップサーバ21が受け付けたクライアント10からのコンテンツ要求に対する許可情報として機能するトランザクションID (TID) の発行処理、コンテンツダウンロード許可情報の発行処理を行なう。また、管理システム31は、ライセンスサーバ22に対して、コンテンツの利用権情報としての利用権データUsage Right) の発行許可を行なう。これらの処理の詳細は、後段で説明する。

【0039】

なお、クライアント10は、ライセンスサーバ22からの利用権の取得、コンテンツサーバ23からのコンテンツ取得を、クライアントアプリケーション12の制御の下に実行し、ショップサーバ21の提供する情報の閲覧および決済処理は、クライアントアプリケーション12の制御の下にブラウザ11を起動して実行する。

【0040】

図1には、クライアントおよび各サーバを1つずつ示してあるが、これらは例えばインターネット等の通信網上に多数接続され、クライアントは、様々なショップサーバに接続し、各ショップサーバで提供するコンテンツを自由に選択し、選択したコンテンツを格納したコンテンツサーバからコンテンツを取得し、取得したコンテンツの利用権を発行するライセンスサーバを選択して、その選択されたライセンスサーバから利用権を取得する。

【0041】

コンテンツは、暗号化コンテンツとしてコンテンツサーバ23からクライアント10に提供される。さらに、ライセンスサーバ22からクライアント10に対しては、コンテンツに対応するコンテンツ利用権情報が提供され、クライアント10のクライアントアプリケーション12が、利用権情報を検証し、利用権があると判定された場合に暗号化コンテンツを復号して利用する。

【0042】

クライアント10は、コンテンツ利用権に基づくコンテンツ利用を可能とするための鍵情報として、有効化キーブロック (EKB: Enabling Key Block)、デバイス・ノード・キー (DNK: Device Node Key) 等の鍵データを保持する。有効化キーブロック (EKB: Enabling Key Block)、デバイス・ノード・キー (DNK: Device Node Key) は、コンテンツの利用を正当なコンテンツ利用権を有するユーザデバイスにおいてのみ暗号化コンテンツを復号して利用可能とするためのコンテンツ利用に必要な暗号鍵を取得するための鍵データである。EKB, DNKについては、後段で説明する。

【0043】

13

コンテンツサーバ23は、コンテンツを暗号化して、暗号化コンテンツをクライアント10に提供する。さらに、ライセンスサーバ22は、コンテンツ利用条件に基づいて利用権情報(Usage Right)を生成してユーザデバイス30に提供する。さらに、管理システム31の提供するデバイスノードキー(DNK: Device Node Key)、有効化キーブロック(EKB: Enabling Key Block)に基づいてサービスデータを生成してクライアント10に提供する。サービスデータは、暗号化コンテンツの復号処理の際に必要なサービス・デバイスノードキー(SDNK)を持つ有効化キーブロック(EKB)を含む。

【0044】

なお、コンテンツの利用条件には、利用期間の限定条件、コピーの回数制限、さらにコンテンツを同時に利用することができるポータブルメディア(PM: Portable Media)の数(いわゆるチェックアウト(Check-out)数に対応)の制限等がある。ポータブルメディア(PM: Portable Media)は例えばフラッシュメモリ、または小型HD、光ディスク、光磁気ディスク、MD(Mini Disk)等、ポータブルデバイスにおいて利用可能な記憶媒体である。

【0045】

次に、図2を参照して、クライアント10、ショップサーバ21、ライセンスサーバ22、コンテンツサーバ23、管理システム31として機能可能な情報処理装置の構成例を示す。これらの各システムはCPUを持つ例えばPC、サーバ等のシステムにそれぞれの処理に応じた処理プログラムを格納することで実現される。

【0046】

まず、図2を用いて各システムの構成例について説明する。CPU(Central Processing Unit)101は、ROM(Read Only Memory)102に記憶されている各種プログラム、あるいは、記憶部108に格納され、RAM(Random Access Memory)103にロードされたプログラムに従って各種処理を実行する。タイマ100は計時処理を行ない、クロック情報をCPU101に供給する。

【0047】

ROM(Read Only Memory)102は、CPU101が使用するプログラムや演算用のパラメータ、固定データ等を格納する。RAM(Random Access Memory)103は、CPU101の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を格納する。これら各素子はCPUバスなどから構成されるバス111により相互に接続されている。

【0048】

14

暗号化復号部104は、コンテンツの暗号化、復号処理、デバイスノードキー(DNK: Device Node Key)、有効化キーブロック(EKB: Enabling Key Block)の適用処理として、例えばDES(Data Encryption Standard)の暗号化アルゴリズムを適用した暗号処理、MAC生成、検証処理等を実行する。さらに、他の接続装置との間で実行されるコンテンツあるいはライセンス情報の送受信時の認証およびセッションキー共有処理等、各種暗号処理を実行する。

【0049】

コーデック部105は、例えばATRAC(Adaptive Transform Acoustic Coding)3方式、MPEG、JPEG方式等、各種方式のデータエンコード処理、デコード処理を実行する。処理対象データは、バス111、入出力インタフェース112、ドライブ110を介してリムーバブル記憶媒体121からまたは通信部109を介して入力する。また処理後のデータは、必要に応じて、リムーバブル記憶媒体121に格納し、または通信部109を介して出力する。

【0050】

入出力インタフェース112には、キーボード、マウス等の入力部106、CRT、LCD等のディスプレイ、スピーカ等からなる出力部107、ハードディスク等の記憶部108、モデム、ターミナルアダプタ等によって構成される通信部109が接続され、例えばインターネット等の通信網を介したデータ送受信を行なう。

【0051】

30 [2. キー配信構成としてのツリー(木)構造について]

次に、正当なコンテンツ利用権を有するクライアントにおいてのみコンテンツを利用可能とするための、ブロードキャストエンクリプション(Broadcast Encryption)方式の一態様であるツリー構成によるデバイスとキーの管理構成について説明する。

【0052】

40 図3の最下段に示すナンバ0~15がコンテンツ利用を行なうクライアントとしてのユーザデバイスである。すなわち図3に示す階層ツリー(木)構造の各葉(リーフ: leaf)がそれぞれのデバイスに相当する。

【0053】

50 各デバイス0~15は、製造時あるいは出荷時、あるいはその後において、図3に示す階層ツリー(木)構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーからなるキーセット(デバイスノードキー(DNK: Device Node Key))をメモリに格納する。図3の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキ

15

一であり、最上段のKR（ルートキー）から、最下段から2番目の節（ノード）に記載されたキー：KR～K111をノードキーとする。

【0054】

図3に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図3のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0055】

また、図3のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【0056】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図3のツリー中に複数存在する。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【0057】

なお、ノードキー、リーフキーは、ある1つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよ

16

い。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行する。

【0058】

このツリー構造において、図3から明らかなように、1つのグループに含まれる3つのデバイス0、1、2、3はデバイスノードキー（DNK：Device Node Key）として共通のキーK00、K0、KRを含むデバイスノードキー（DNK：Device Node Key）を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00は、デバイス0、1、2、3に共通する保有キーとなる。また、新たなキーKnewをノードキーK00で暗号化した値Enc（K00、Knew）を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc（K00、Knew）を解いて新たなキーKnewを得ることが可能となる。なお、Enc（Ka、Kb）はKbをKaによって暗号化したデータであることを示す。

【0059】

また、ある時点tにおいて、デバイス3の所有する鍵：K0011、K001、K00、K0、KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0、1、2、3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K001、K00、K0、KRをそれぞれ新たな鍵K（t）001、K（t）00、K（t）0、K（t）Rに更新し、デバイス0、1、2にその更新キーを伝える必要がある。ここで、K（t）aaaは、鍵Kaaaの世代（Generation）：tの更新キーであることを示す。

【0060】

更新キーの配布処理について説明する。キーの更新は、例えば、図4（A）に示す有効化キーブロック（EKB：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0、1、2に供給することによって実行される。なお、有効化キーブロック（EKB）は、図3に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（EKB）は、キー更新ブロック（KRB：Key Renewal Block）と呼ばれることもある。

【0061】

図4(A)に示す有効化キープブロック(EKB)には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図4の例は、図3に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図3から明らかなように、デバイス0, デバイス1は、更新ノードキーとしてK(t)00, K(t)0, K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK

【0062】

図4(A)のEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001を得ることができる。また、復号により得たK(t)001を用いて、図4(A)の下から2段目の暗号化キーEnc(K(t)001, K(t)00)を復号可能となり、更新ノードキーK(t)00を得ることができる。以下順次、図4(A)の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0、図4(A)の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号しK(t)Rを得る。一方、デバイスK0000, K0001は、ノードキーK0000は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t)00, K(t)0, K(t)Rである。デバイスK0000, K0001は、図4(A)の上から3段目の暗号化キーEnc(K0000, K(t)00)を復号しK(t)00、を取得し、以下、図4(A)の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0、図4(A)の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号しK(t)Rを得る。このようにして、デバイス0, 1, 2は更新した鍵K(t)Rを得ることができる。なお、図4(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0063】

図3に示すツリー構造の上位段のノードキー：K(t)0, K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図4(B)の有効化キープブロック(EKB)を用いることで、更新ノードキーK(t)00をデバイス0, 1, 2に配布することができる。

【0064】

図4(B)に示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図3に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のコンテンツキーK(t)conが必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキーK00を更新したK(t)00を用いて新たな共通の更新コンテンツキー：K(t)conを暗号化したデータEnc(K(t), K(t)con)を図4(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0065】

すなわち、デバイス0, 1, 2はEKBを処理して得たK(t)00を用いて上記暗号文を復号すれば、t時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツキーK(t)conを得ることが可能になる。

【0066】

[3. EKBを使用したキーの配布]

図5に、t時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツキーK(t)conを得る処理例として、K(t)00を用いて新たな共通のコンテンツキーK(t)conを暗号化したデータEnc(K(t)00, K(t)con)と図4(B)に示すEKBとを記録媒体を介して受領したデバイス0の処理例を示す。すなわちEKBによる暗号化メッセージデータをコンテンツキーK(t)conとした例である。

【0067】

図5に示すように、デバイス0は、記録媒体に格納されている世代：t時点のEKBと自分があらかじめ格納しているノードキーK000を用いて上述したと同様のEKB処理により、ノードキーK(t)00を生成する。さらに、復号した更新ノードキーK(t)00を用いて更新コンテンツキーK(t)conを復号して、後にそれを使用するために自分だけが持つリーフキーK000で暗号化して格納する。

【0068】

[4. EKBのフォーマット]

図6に有効化キープブロック(EKB)のフォーマット例を示す。バージョン201は、有効化キープブロック(EKB)のバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キープブロック(EKB)の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ203は、有効化キープブロック(EKB)中のデータ部の位置を示すポインタであり、タグポインタ204はタグ部の位置、署名ポインタ205は署名の位置を示すポインタである。

50 【0069】

データ部206は、例えば更新するノードキーを暗号化したデータを格納する。例えば図5に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0070】

タグ部207は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図7を用いて説明する。図7では、データとして先に図4(A)で説明した有効化キーブロック(EKB)を送付する例を示している。この時のデータは、図7の表(b)に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーK(t)Rが含まれているので、トップノードアドレスはKRとなる。このとき、例えば最上段のデータEnc(K(t)0, K(t)R)は、図7の(a)に示す階層ツリーに示す位置にある。ここで、次のデータは、Enc(K(t)00, K(t)0)であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは(左(L)タグ, 右(R)タグ)として設定される。最上段のデータEnc(K(t)0, K(t)R)の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図7(c)に示すデータ列、およびタグ列が構成される。

【0071】

タグは、データEnc(Kxxx, Kyyy)がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータEnc(Kxxx, Kyyy)・・・は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図4で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、
0: Enc(K(t)0, K(t)root)
00: Enc(K(t)00, K(t)0)
000: Enc(K(t)000, K(T)00)
・・・のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0072】

図6に戻って、EKBフォーマットについてさらに説明する。署名(Signature)208は、有効化キーブロック(EKB)を発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署

名である。EKBを受領したデバイスは署名検証によって正当な有効化キーブロック(EKB)を発行者が発行した有効化キーブロック(EKB)であることを確認する。

【0073】

[5. ツリーのカテゴリ分類]

ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【0074】

図8に階層ツリー構造のカテゴリの分類の一例を示す。図8において、階層ツリー構造の最上段には、ルートキーKroot301が設定され、以下の中間段にはノードキー302が設定され、最下段には、リーフキー303が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【0075】

ここで、一例として最上段から第M段目のあるノードをカテゴリノード304として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【0076】

例えば図8の第M段目の1つのノード305にはカテゴリ[メモリスティック(商標)]が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード305以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【0077】

さらに、M段から数段分下位の段をサブカテゴリノード306として設定することができる。例えば図に示すようにカテゴリ[メモリスティック]ノード305の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、[再生専用器]のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード306以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード307が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる[PHS]ノード308と[携帯電話]ノード309を設定することができる。

【0078】

さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の

21

単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キープロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0079】

このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キープロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【0080】

本発明のシステムにおいては、図9に示されるように、ツリー構成のシステムで、キー管理が行われる。図9の例では、8+24+32段のノードがツリー構造とされ、ルートノードから下位の8段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム（Tシステムと称する）が対応する。

【0081】

すなわち、このTシステムのノードよりさらに下の階層の24段のノードに対応するキーが、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。この例の場合、これにより、2²⁴（約16メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の32段の階層により、2³²（約4ギガ）のユーザ（あるいはユーザデバイス）を規定することができる。最下段の32段のノードからTシステムのノードまでのパス上の各ノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリーフに対応するIDがリーフIDとされる。

【0082】

例えば、コンテンツを暗号化したコンテンツキーは更新

22

されたルートキーKR'によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、EKB内に配置される。EKBにおける末端から1つ上の段の更新ノードキーはEKBの末端のノードキーあるいはリーフキーによって暗号化され、EKB内に配置される。

【0083】

ユーザデバイスは、サービスデータに記述されているDNKのいずれかのキーを用いて、コンテンツデータとともに配布されるEKB内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、EKB内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルートキーKR'を得ることができる。

【0084】

上述したように、ツリーのカテゴリ分類により、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化キープロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

【0085】

さらに、上述のツリー構成のデバイス管理によるEKB配信システムを適用して、複数のカテゴリに基づくEKB配信構成を採用したコンテンツ配信および利用形態について説明する。

【0086】

図10を参照して2つのカテゴリについて説明する。図10に示すように、ルートノード350の下段にTシステムノード351を設定し、その下段にTサービスノード352、およびTハードノード353を設定する。Tハードノード353を頂点としたツリーは、ユーザデバイス機器自体をリーフ355として設定し、機器を対象として発行するハード対応EKB[EKB(H)]を配信するカテゴリツリーである。一方、Tサービスノード352を頂点としたツリーは、ユーザデバイス機器に提供するサービスに対応して発行するサービス対応EKB[EKB(S)]を配信するカテゴリツリーである。

【0087】

ハード対応EKB[EKB(H)]、サービス対応EKB[EKB(S)]とも、それぞれ正当な権限を持つデバイスに対して与えられるDNK(Device Node Key)すなわち、リーフからTシステムのノードまでのパス上の各ノードに対応するキーを有することで、各EKBの復号が可能となる。

【0088】

[6. コンテンツ購入および試聴処理]

次に、クライアントがコンテンツを購入または試聴する際の処理の詳細について、図11以下を参照して説明する。

【0089】

図11は、クライアントアプリケーション、ブラウザを有するPC等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるコンテンツ購入処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

【0090】

まず、クライアント側において、コンテンツの購入を行なおうとするユーザは、自己のPC等の通信可能な情報処理装置にURLを指定(ステップ(1))し、ブラウザが介してショップサーバの提示するコンテンツリスト画面(ショップページ)を読み出し(ステップ(2))て、ディスプレイに表示(ステップ(3))する。

【0091】

クライアントは、ショップサーバの提示するコンテンツリストからコンテンツを選択して、さらに、購入または試聴どちらかの指定(ステップ(4))を行なって、ブラウザを介してショップサーバに要求データを送信(ステップ(5))する。要求データには、コンテンツID(CID)、ショップサーバ識別子(ShopID)、および購入または試聴どちらかの指定データが含まれる。

【0092】

ショップサーバは、クライアントからのコンテンツ購入、または試聴要求を受信すると、管理システムに対して、コンテンツの提供の可否判定を要求(ステップ(6))する。この判定要求には、コンテンツID(CID)、ショップサーバ識別子(ShopID)が含まれる。

【0093】

管理システムは、コンテンツの提供の可否判定要求を受信すると、トランザクションID(TID)の発行処理(ステップ(7))を実行する。トランザクションID(TID)の発行処理の詳細を図12のフローを参照して説明する。

【0094】

管理システムは、まず、ステップS101において、乱数を発生し、発生乱数に基づいて、トランザクションID(TID)を生成する。次に、ステップS102において、生成したトランザクションID(TID)と、ショップサーバから指定されたコンテンツID(CID)とを対応付けてトランザクションデータとして記憶部に格納する。次に、生成したトランザクションID(TID)をショップサーバに対して出力、発行する。

【0095】

図11のシーケンス図に戻る。管理システムは、トランザクションID(TID)の生成後、生成したトランザクションID(TID)と価格情報をTID情報としてショップサーバに送信(ステップ(8))する。ただし、価格情報は、コンテンツ購入時においてのみ要求される情報であり、コンテンツ試聴処理に際しては、含まれない。TID情報を受信したショップサーバは、クライアントからの要求がコンテンツ購入である場合に、TID情報に含まれる価格に基づいて、課金処理(ステップ(9))を実行する。

【0096】

クライアントからの要求がコンテンツ購入ではなく、コンテンツ試聴要求である場合には、この課金処理(ステップ(9))は省略される。

【0097】

次に、図13のシーケンス図を参照して継続する処理について説明する。ショップサーバは、コンテンツ購入処理においては、課金が行われたことを条件として、またコンテンツ試聴処理においては、管理システムからのTID情報の受信を条件として、購入または試聴要求対象のコンテンツのダウンロード許可要求を管理システムに対して送信(ステップ(10))する。

【0098】

管理システムは、ダウンロード許可要求を受信すると、ダウンロード許可要求検証処理(ステップ(11))を実行する。ダウンロード許可要求検証処理の詳細を図14のフローを参照して説明する。

【0099】

管理システムは、まず、ステップS201において、受信したダウンロード許可要求に含まれるトランザクションID(TID)と、先に生成し、記憶部に格納したトランザクションID(TID)とを照合し、さらにステップS202において、照合の成立したトランザクションID(TID)に対応して記録されたコンテンツID(CID)を取得し、ステップS203において、CIDに対応するコンテンツのダウンロード許可を発行する。

【0100】

図13のシーケンス図に戻り、説明を続ける。管理システムは、ダウンロード許可要求検証処理(ステップ(11))の後、コンテンツのダウンロード許可をショップサーバに対して発行(ステップ(12))する。ダウンロード許可には、トランザクションID(TID)、コンテンツサーバURL(C-URL)、ライセンスサーバURL(L-URL)、コンテンツID(CID)、利用権情報ID(UID)、商品(コンテンツ)URL(S-URL)、サービスIDが含まれる。

【0101】

ショップサーバは、管理システムからダウンロード許可を受信すると、クライアントアプリケーションにおける

コンテンツの利用（再生処理等）プログラムを起動させるための起動ファイルを生成してクライアントのブラウザを介してクライアントアプリケーションに対して送付する。

【0102】

起動ファイルの例を図15を参照して説明する。起動ファイル360は、先に管理システムが生成したトランザクションID（TID）、クライアントが購入あるいは試聴するコンテンツID（CID）、管理システムが生成したダウンロード許可情報に含まれる利用権情報ID（UID）、管理システムが生成したダウンロード許可情報に含まれるサービスID、ライセンスサーバURL、商品（コンテンツ）URL、さらに、処理が購入であるか試聴であるかの識別データが含まれる。

【0103】

なお、処理が購入であるか試聴であるかの識別データとしては、起動ファイルに設定される拡張子を購入であるか試聴であるかによって区別して設定し、これをクライアントアプリケーションが判別して、それぞれのアプリケーションを起動するようにしてもよい。

【0104】

クライアントアプリケーションは、起動ファイルに応じて、アプリケーションを起動（ステップ（15））する。

【0105】

クライアントアプリケーションにおいて実行するアプリケーション起動処理について、図16を参照して説明する。ステップS301において、まず、起動ファイルに設定されたサービスID対応のサービスデータをクライアントシステムとしての情報処理装置に格納されているか否かを判定する。

【0106】

サービスデータは、クライアントが各種のサービス、例えばコンテンツ利用サービスを受領したい場合、ライセンスサーバから受領するもので、例えば特定のサービスプロバイダの提供サービスの一括したサービス利用権を認めるデータである。図17（a）にサービスデータのデータ構成例を示す。

【0107】

図17（a）に示すように、サービスデータ370には、EKB配信ツリーにおいて設定されるクライアントに固有のリーフID、サービス識別子としてのサービスID、さらにデバイスノードキー（DNK）をルートキー（Kroot）で暗号化したデータ、E（Kroot, DNK）が含まれる。サービスデータを受領するためには、クライアントは、ライセンスサーバに対する登録処理が必要とされる。登録処理は、図13に示す処理ステップ（15）、（16）の処理に対応する。

【0108】

図16に示すステップS301において、サービスID

対応のサービスデータを保有していないと判定すると、ステップS302において登録処理を実行して、サービスデータを受領する。

【0109】

さらに、この登録処理時に、デフォルト利用権情報がライセンスサーバからクライアントに対して発行される。利用権情報は、通常は、購入コンテンツの利用条件を格納し、コンテンツの購入に対応して発行されるものであるが、デフォルト利用権情報は、コンテンツの購入を条件として発行するものではなく、クライアントの登録処理、あるいはサービスデータの発行処理を条件として発行する。このデフォルト利用権情報は、後段で説明するコンテンツの試聴処理の際の有効なコンテンツ利用権情報として適用される。

【0110】

図17（b）に利用権情報のデータ構成例を示す。図17（b）に示すように、利用権情報371には、利用権情報識別子としての利用権情報ID、発行日時情報としてのタイムスタンプ、クライアントに固有のリーフID、コンテンツ対応である場合は、コンテンツID、さらに、利用条件対象コンテンツ種別情報が格納される。

【0111】

デフォルト利用権情報の場合は、特定の購入コンテンツに対応して発行されるものではないため、コンテンツIDは省略、あるいは試聴可能なコンテンツに共通なIDが設定される。また、利用条件対象コンテンツ種別情報として、例えば試聴フラグがオン（ON）として設定されたコンテンツについての利用が許可される設定とする。コンテンツ372には図17（c）に示すように、試聴フラグ373が設定され、試聴フラグ373がオン（ON）の設定コンテンツであれば、試聴が許可されたコンテンツであることを示し、試聴フラグがオフ（OFF）の設定コンテンツであれば、試聴が許可されていないコンテンツであることを示す。

【0112】

クライアントアプリケーションは、試聴コンテンツ再生時には、デフォルト利用権情報を参照して、再生許可の有無を判定するとともに、コンテンツのフラグの検証を実行して、コンテンツの再生を行なうことになる。この処理については、後段で説明する。

【0113】

図16の処理フローに戻りアプリケーション起動処理の処理手順について説明する。ステップS302において、登録処理、すなわちライセンスサーバからのサービスデータ、デフォルト利用権情報の取得が終了すると、ステップS303において、ショップサーバから受信した起動ファイルが、購入用アプリケーションの起動ファイルであるか、試聴用アプリケーションの起動ファイルであるかを判別する。購入用アプリケーションの起動ファイルである場合は、ステップS304に進み購入用ア

アプリケーションを実行し、試験用アプリケーションの起動ファイルである場合は、ステップS305に進み試験用アプリケーションを実行する。

【0114】

次に、購入用アプリケーションの実行シーケンスについて、図18のシーケンス図を参照して説明する。

【0115】

購入処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行(ステップ21)する。これは、先にクライアントが購入要求を行なったコンテンツであり、利用権情報(図17(b)参照)に記録されたコンテンツID(CID)に対応するコンテンツである。クライアントアプリケーションは、コンテンツID(CID)によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

【0116】

コンテンツサーバは、コンテンツダウンロード要求を受信すると、CIDに対応するコンテンツ情報をクライアントに送信(ステップ22)する。このコンテンツ情報は、暗号化コンテンツを含み、図17(c)に示すように、コンテンツキー:Kcで暗号化されたコンテンツデータ:Enc(Kc, Content)、コンテンツキー:Kcをルートキー:Krootで暗号化したデータ:Enc(Kroot, Kc)、さらに:ルートキー:Krootを取得するためのEKB、さらに試験フラグデータ、サービスID等の情報が付加されたファイルである。

【0117】

コンテンツ情報を受領したクライアントは、受信コンテンツに対応する利用権情報(Usage Right)の取得要求をライセンスサーバに対して送信(ステップ23)する。この要求には、先にショップサーバから受領した起動ファイル(図15参照)中に含まれる利用権情報ID(UID)、クライアント識別データとしてのリーフID、および先にショップサーバから受領した起動ファイル(図15参照)中に含まれるトランザクションID(TID)が含まれる。

【0118】

ライセンスサーバは、利用権情報(Usage Right)の取得要求を受信すると、管理システムに対して、注文照会処理(ステップ24)を行なう。この要求には、利用権情報ID(UID)、トランザクションID(TID)が含まれる。注文照会を受信した管理サーバは、注文照会応答として、利用権情報ID(UID)に対応する利用条件を設定した応答情報をライセンスサーバに送信(ステップ25)する。

【0119】

応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報(Usage Right

t)を生成して、クライアントに対して発行(ステップ26)する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェックアウト処理等の各種処理の許可情報によって構成される。

【0120】

利用権情報(Usage Right)を受信したクライアントは、先にコンテンツサーバから受信したコンテンツについて、利用権情報(Usage Right)に記録された利用条件に基づいてコンテンツの利用が可能となる。ユーザからコンテンツID(CID)、利用権情報(Usage Right)IDを指定したコンテンツ再生要求(ステップ27)があると、クライアントアプリケーションは、利用条件に従ったコンテンツ再生を実行(ステップ28)する。

【0121】

基本的なコンテンツ再生処理の手順について、図19を参照して説明する。前述の説明から理解されるように、コンテンツサーバ382からクライアント383に対してコンテンツが提供されるとともに、ライセンスサーバ381からクライアント383にライセンスとして、サービスデータ、利用権情報(Usage Right)が与えられる。

【0122】

コンテンツは、コンテンツキー:Kcにより、暗号化されており(Enc(Kc, Content)、コンテンツキーKcは、EKBから取得可能なルートキーKrootから得られるキーである。

【0123】

クライアント383は、ライセンスサーバから受領したサービスデータからデバイスノードキー(DNK)を取得し、取得したDNKに基づいてコンテンツファイルのEKBを復号して、ルートキー:Krootを取得し、さらに、取得したルートキー:Krootを用いて、Enc(Kroot, Kc)を復号してコンテンツキー:Kcを取得し、取得したコンテンツキー:Kcをにより暗号化コンテンツ:Enc(Kc, Content)の復号処理を実行してコンテンツを取得し、再生する。

【0124】

サービスデータ、利用権情報(Usage Right)と対応付けたコンテンツ再生処理の詳細について、図20を参照して説明する。

【0125】

図20は、ハード対応EKB[EKB(H)]、サービス対応EKB[EKB(S)]を適用したコンテンツの復号処理に基づくコンテンツ利用処理シーケンスを説明した図である。

【0126】

図20に示すサービスデータ401、および利用権情報403は、ライセンスサーバから受領するデータであ

り、暗号化コンテンツファイル402はコンテンツサーバから受領するデータである。サービスデータ401は、リーフ識別子としてのリーフID、適用するEKBのバージョン、さらに、サービス対応EKB[EKB(S)]の復号に必要なサービス対応デバイスノードキー(SDNK)を、ハード対応カテゴリツリーに対応して設定されるルートキーKroot'によって暗号化したデータE(Kroot', SDNK)を格納している。

【0127】

暗号化コンテンツファイル402は、サービス対応のカテゴリツリーに対応して設定されるルートキーKrootを格納したサービス対応EKB[EKB(S)]、ルートキーKrootでコンテンツID(CID)と、コンテンツ暗号処理および復号処理に適用するコンテンツキー(Kc)とを暗号化したデータE(Kroot, CID+Kc)、および、コンテンツ(Content)をコンテンツキーKcで暗号化したデータE(Kc, Content)を含むファイルである。

【0128】

また、利用権情報403は、リーフIDと、コンテンツの利用条件情報を格納したデータである。コンテンツの利用条件情報には、コンテンツに対応して設定される利用期間、利用回数、コピー制限等の様々な利用条件が含まれる。利用権情報403を受領したユーザデバイスは、利用権情報をコンテンツに対応するセキュリティ情報として格納するか、あるいは、コンテンツの索引データとしてのAVインデックスファイル内に格納する。

【0129】

例えば、PC等の大容量の記憶手段を有し、プロセッサ等の処理能力が高いユーザデバイスにおいては、利用権情報をコンテンツに対応するセキュリティ情報として格納することが可能であり、すべての利用権情報を格納して、コンテンツ利用の際にすべての利用権情報を参照した処理を行なうことが好ましい。一方、大容量の記憶手段を持たず、またプロセッサ等の処理能力が低いポータブルデバイス(PD)等のユーザデバイスにおいては、選択された情報からなる利用権情報403をコンテンツの索引データとしてのAVインデックスファイル内に格納して、コンテンツ利用の際にAVインデックスファイル内の利用条件情報を参照した処理を行なう等の処理が可能である。

【0130】

ユーザデバイスは、図20に示すステップS501において、ハード対応のデバイスノードキー(HDNK)412を適用して、ハード対応のEKB(H)411の復号処理を実行し、EKB(H)411から、ハード対応カテゴリツリーに対応して設定されるルートキーKroot'を取得する。DNKを適用したEKBの処理は、先に図5を参照して説明した手法に従った処理となる。

【0131】

次に、ステップS502において、EKB(H)から取り出したルートキーKroot'を用いて、サービスデータ401内の暗号化データE(Kroot', SDNK)の復号処理を実行し、サービス対応EKB[EKB(S)]の処理(復号)に適用するデバイスノードキー(SDNK)を取得する。

【0132】

次に、ステップS503において、サービスデータから取り出したデバイスノードキー(SDNK)を用いて、暗号化コンテンツファイル402内に格納されたサービス対応EKB[EKB(S)]の処理(復号)を実行し、サービス対応EKB[EKB(S)]内に格納されたサービス対応カテゴリツリーに対応して設定されるルートキーKrootを取得する。

【0133】

次に、ステップS504において、サービス対応EKB[EKB(S)]から取り出したルートキーKrootを用いて、暗号化コンテンツファイル402内に格納された暗号化データE(Kroot, CID+Kc)の復号処理を実行し、コンテンツID(CID)と、コンテンツキー(Kc)を取得する。

【0134】

次に、ステップS505において、暗号化コンテンツファイル402から取り出したコンテンツID(CID)と、利用権情報内に格納されたコンテンツIDのマッチング(照合)処理を実行する。マッチング処理により、コンテンツの利用が可能であることが確認されると、ステップS506において、暗号化コンテンツファイル402から取り出したコンテンツキー(Kc)を適用して、暗号化コンテンツファイル402に格納された暗号化コンテンツE(Kc, Content)を復号してコンテンツの再生を行なう。

【0135】

上述したように、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB[EKB(H)]と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB[EKB(S)]をそれぞれ個別にユーザに対して提供し、それぞれのEKBに対する正当なDNKを有するユーザのみがサービスの利用を行なうことが可能となる。

【0136】

サービス対応EKB[EKB(S)]を復号するためのDNK、すなわちSDNKは、コンテンツに対応したサービスデータ401として提供可能であり、またSDNKを正当なハードウェア対応のDNK、すなわちHDNKを有する機器のみが取得可能なハード対応カテゴリツリーに対応して設定されるルートキーKroot'を適用して暗号化した構成としたので、正当なHDNKを有

するユーザデバイスのみが、SDNKを取得でき、サービスが利用となる。

【0137】

また、コンテンツ利用において、暗号化コンテンツファイル402から取得されるコンテンツ識別子(CID)と、利用権情報から取得されるCIDとのマッチング処理を実行する構成としたので、利用権情報403を取得してCID情報を格納していることがコンテンツ再生プロセスの必須要件とすることが可能となり、利用条件に従ったコンテンツ利用が実現される。

【0138】

次に、クライアントアプリケーションの処理が試聴処理の実行アプリケーションである場合の処理について、図21のシーケンス図を参照して説明する。

【0139】

試聴処理の場合、コンテンツ購入処理と同様、コンテンツ情報ファイル(図19参照)を取得してクライアントシステムの記憶部に格納し、その後、購入コンテンツと同様の処理によって再生することも可能であるが、記憶部に格納することなく、ストリーミング再生処理を実行する例について、図21を参照して説明する。

【0140】

ストリーミング試聴処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行(ステップ(31))する。これは、先にクライアントが試聴要求を行なったコンテンツである。クライアントアプリケーションは、コンテンツID(CID)によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

【0141】

コンテンツサーバは、ストリーミング再生の場合には、コンテンツの部分データ(コンテンツパート)を次々にクライアントに対して送信(ステップ(32))する。コンテンツパートを受信したクライアントは、受信コンテンツに対する再生処理を実行(ステップ(33))し、後続のコンテンツパートの要求をコンテンツサーバに送信する。この処理を連続して実行することによりストリーミング再生が行なわれる。

【0142】

試聴再生処理の手順について、図22のフローを参照して説明する。ステップS701において、クライアントアプリケーションは、コンテンツサーバから受信した試聴コンテンツファイル中からサービスIDを取得する。

【0143】

次にステップS702において、抽出したサービスIDに対応するデフォルト利用権情報(Default Usage Right)(図17(b)参照)の有無を判定する。デフォルト利用権情報は、クライアントの登録処理時に、サービスデータ(図17(a)参照)と

もに、ライセンスサーバから送信される利用権情報であり、購入コンテンツに対応して発行される利用権情報と異なり、試聴可能なコンテンツに対して利用される利用権情報である。

【0144】

コンテンツ試聴においては、デフォルト利用権情報(Default Usage Right)を保有することが試聴実行許可条件であり、デフォルト利用権情報を保有していない場合は、ステップS705に進み、エラーとしてコンテンツ再生が実行されず処理を終了する。

【0145】

デフォルト利用権情報(Default Usage Right)が格納されている場合は、ステップS703において、デフォルト利用権情報を検証し、利用権情報の記録を確認する。デフォルト利用権情報には、例えば試聴フラグオンのコンテンツの試聴許可、あるいは試聴可能なコンテンツID情報が格納されており、これらの情報を取得する。

【0146】

次にステップS704において、デフォルト利用権情報(Default Usage Right)の利用条件に基づいてコンテンツが再生される。なお、再生処理は、前述の図19、図20を参照して説明したように、コンテンツサーバから受信する暗号化コンテンツの復号処理を伴う再生処理となる。

【0147】

なお、コンテンツの購入処理を伴わない試聴処理においても、図20を参照して説明した購入コンテンツの再生と同様、EKB処理に基づくキー取得処理によってコンテンツ復号用のキーを取得することが必要となる。例えば、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB[EKB(H)]と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB[EKB(S)]に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴においても再生権限を限定した範囲として設定可能となる。

【0148】

上述したように、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報(Default Usage Right)を取得し、コンテンツの購入処理を伴わない、試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生を可能とした構成であるので、ユーザは、コンテンツの購入を実行することなく、コンテンツの試聴再生が可能となり、また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

【0149】

なお、図21のシーケンス図では、ストリーミング再生の例を示したが、試聴データをクライアントの記憶媒体に格納し、再生時に、デフォルト利用権情報(Default Usage Right)の有無を判定して、デフォルト利用権情報の記録に基づいて再生を行なう構成とすることも可能である。

【0150】

[7. バックアップ/リストア処理]

次にクライアントが購入したコンテンツまたはコンテンツ利用権情報についてのバックアップ処理、リストア処理について説明する。

【0151】

リストア処理は、クライアントのコンテンツ購入時、あるいは購入後の処理として実行されるコンテンツ対応のライセンス情報、すなわちサービスデータ、利用権情報の再取得、格納処理、あるいはコンテンツの再取得処理として実行される。

【0152】

処理態様としては、サービスデータ、利用権情報、コンテンツのいずれかの再取得、あるいはこれらの全データの再取得が可能である。以下に説明する実施例においては、サービスデータ、利用権情報、コンテンツ全データの再取得、格納処理シーケンス例を説明するが、必ずしもこれら全データを再取得する処理に限らず、いずれかのデータのみを選択的に再取得することも可能である。

【0153】

図23以下を参照して、バックアップ/リストア処理の詳細について説明する。図23は、クライアントアプリケーション、ブラウザを有するPC等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるバックアップ/リストア処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

【0154】

クライアントは、前述したコンテンツ購入処理に従って、正規にコンテンツ購入を行なったものとする。図23に示すシーケンスは、コンテンツ購入に続いて実行されるシーケンスである。

【0155】

コンテンツ購入処理を実行したクライアントは、バックアップ/リストアデータの取得のためのデータファイルとしてのリストア処理要求ファイル[restore.dat]を生成(ステップ50)する。リストア処理要求ファイル[restore.dat]の構成を図24に示す。

【0156】

図24に示すように、リストア処理要求ファイル[restore.dat]は、EKB配信ツリーにおけるク

ライアント識別データとしてのリーフIDと、ハッシュ(hash)値、例えばMAC(Message Authentication Code)からなる検証データによって構成される。クライアントアプリケーションは、管理システムと共有する秘密の鍵を適用してリーフIDに基づく検証用データとしてのハッシュ値あるいはMACを算出し、リーフIDと検証用データからなるリストア処理要求ファイル[restore.dat]を生成する。

【0157】

メッセージ認証符号(MAC: Message authentication Code)は、データの改竄検証用のデータとして生成されるものである。DES暗号処理構成を用いたMAC値生成例を図25に示す。図25の構成に示すように対象となるメッセージを8バイト単位に分割し、(以下、分割されたメッセージをM1、M2、・・・、MNとする)、まず、初期値(Initial Value(以下、IVとする))とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返す、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号(MAC(Message Authentication Code))となる。

【0158】

MAC値は、その生成元データが変更されると、異なる値になり、検証対象のデータ(メッセージ)に基づいて生成したMACと、記録されているMACとの比較を行い、一致していれば、検証対象のデータ(メッセージ)は変更、改竄がなされていないことが証明される。

【0159】

図23のシーケンスに戻り説明を続ける。クライアントは、ブラウザを介して管理システムの提供するリストアページにアクセス(ステップ51)し、管理システムは、リストアページをクライアントのブラウザに提示(ステップ52)する。管理システムの提示するリストアページは、リストア処理要求ファイル[restore.dat]のアップロード処理を実行する機能を持つページである。

【0160】

クライアントは、管理システムの提示するリストアページにおいて、クライアントアプリケーションの生成したリストア処理要求ファイル[restore.dat]をアップロードする。リストア処理要求ファイル[restore.dat]は、図24を参照して説明したように、EKB配信ツリーにおけるクライアント識別データとしてのリーフIDと、例えばMAC(Message

e Authentication Code) からなるハッシュ (hash) 値によって構成される。

【0161】

管理システムは、リストア処理要求ファイル [restore.dat] を受信すると、クライアントと共有する秘密鍵を用いて、リーフIDに対するハッシュ値を算出し、算出ハッシュ値と、受信ハッシュ値の照合処理を行ない、受信データの検証 (ステップ (54)) を行なう。算出ハッシュ値と、受信ハッシュ値が適合したことを条件として、バックアップ/リストア用の起動ファイルをクライアントに送信 (ステップ (55)) する。起動ファイルの構成は、先に図15を参照して説明したと同様のファイル構成を持つ。

【0162】

起動ファイルは、ブラウザからクライアントアプリケーションに渡され (ステップ (56))、起動ファイルの記述、あるいは拡張子によって判別選択されるバックアップ/リストア実行プログラムを起動し、リストア処理を実行 (ステップ (57)) する。

【0163】

バックアップ/リストア処理の処理対象としては、サービスデータ、コンテンツ、コンテンツ利用権情報がある。サービスデータは前述したようにライセンスサーバに対する登録処理によって取得可能であり、コンテンツはコンテンツサーバから取得可能である。また、利用権情報は、ライセンスサーバから取得される。バックアップ/リストア処理においても、これらの各データは、それぞれのサーバから取得することになる。

【0164】

まず、図26を参照して、バックアップ/リストア用サービスデータの取得処理について説明する。基本的に、この処理は、先に説明したコンテンツ購入時のクライアント登録処理と同様の手続きに従ったものとなる。

【0165】

まず、クライアントアプリケーションは、登録要求をライセンスサーバに送信 (ステップ (61)) する。この登録要求には、管理システムが生成した起動ファイル中に含まれるトランザクションID (TID) が含まれる。

【0166】

登録要求を受信したライセンスサーバは、トランザクションID (TID) に基づいて、バックアップ/リストア用サービスデータの取得であることを識別し、管理システムに対してサービス事前データ、すなわちサービスデータのバックアップ/リストア用データの割当要求 (ステップ (62)) を行なう。管理システムは、同じトランザクションIDに基づいて処理を実行したクライアント端末があるか否かを管理データに基づいて検証し、ある場合には、これらに対応付けて記憶 (ステップ (63)) する。これは、バックアップ/リストア処理

の処理回数の上限 (例えば3回) を設定し、上限を超える処理要求の場合には、処理を実行しないという設定を可能とするためである。

【0167】

管理データの更新処理を実行した管理システムは、サービス事前データ割当応答をライセンスサーバに送信 (ステップ (64)) する。これは、バックアップ/リストア用サービスデータの発行許可情報として送信されるものである。

【0168】

サービス事前データ割当応答を受信したライセンスサーバは、バックアップ/リストア用サービスデータのクライアントに対する発行処理を実行 (ステップ (65)) する。サービスデータは、先に図17(a)を参照して説明したように、サービスデータ370には、EKB配信ツリーにおいて設定されるクライアントに固有のリーフID、サービス識別子としてのサービスID、さらにデバイスノードキー (DNK) をルートキー (Root) で暗号化したデータ、E (Root, DNK) が含まれる。

【0169】

さらに、この処理時に、デフォルト利用権情報 (図17(b)参照) もライセンスサーバからクライアントに対して発行される。先に説明したように、利用権情報は、通常は、購入コンテンツの利用条件を格納し、コンテンツの購入に対応して発行されるものであるが、デフォルト利用権情報は、コンテンツの購入を条件として発行するものではなく、クライアントの登録処理、あるいはサービスデータの発行処理を条件として発行する。このデフォルト利用権情報は、前述したようにコンテンツの試聴処理の際の有効な利用権情報として適用される。

【0170】

ライセンスサーバからサービスデータ、デフォルト利用権情報を受領したクライアントは、これらのデータをバックアップ用として、記憶手段に格納 (ステップ (66)) する。

【0171】

次に、図27を参照して、コンテンツのバックアップ/リストア処理について説明する。コンテンツのバックアップ/リストア処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行 (ステップ (71)) する。これは、先にクライアントが購入したコンテンツと同一である。クライアントアプリケーションは、コンテンツID (CID) によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

【0172】

コンテンツサーバは、コンテンツダウンロード要求を受信すると、CIDに対応するコンテンツ情報をクライアントに送信 (ステップ (72)) する。このコンテンツ

情報は、暗号化コンテンツを含む情報である。先に図17(c)を参照して説明したように、コンテンツキー：Kcで暗号化されたコンテンツデータ：Enc(Kc, Content)、コンテンツキー：Kcをルートキー：Krootで暗号化したデータ：Enc(Kroot, Kc)、さらに：ルートキー：Krootを取得するためのEKB、さらに試聴フラグデータ、サービスID等の情報が付加されたファイルである。

【0173】

コンテンツ情報を受領したクライアントは、受信コンテンツに対応する利用権情報(Usage Right)の取得要求をライセンスサーバに対して送信(ステップ73)する。この要求には、起動ファイル(図15参照)中に含まれる利用権情報ID(UID)、クライアント識別データとしてのリーフID、トランザクションID(TID)が含まれる。

【0174】

ライセンスサーバは、利用権情報(Usage Right)の取得要求を受信すると、管理システムに対して、注文照会処理(ステップ74)を行なう。この要求には、利用権情報ID(UID)、トランザクションID(TID)が含まれる。注文照会を受信した管理サーバは、注文照会応答として、利用権情報ID(UID)に対応する利用条件を設定した応答情報をライセンスサーバに送信(ステップ75)する。

【0175】

応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報(Usage Right)を生成して、クライアントに対して再発行(ステップ76)する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェックアウト処理等の各種処理の許可情報によって構成される。

【0176】

利用権情報(Usage Right)を受信したクライアントは、先に受信したコンテンツと利用権情報とを記憶手段にバックアップデータとして格納する。

【0177】

なお、バックアップ／リストア処理において、ライセンスサーバが発行する利用権情報は、正規なコンテンツ購入処理に際して発行する利用権情報とは異なる利用条件を設定したものとしてもよい。例えば、正規なコンテンツ購入時に発行する利用権情報に含まれる利用条件より厳しい条件、例えば利用期間の制限、コピー禁止、あるいはチェックアウト禁止といった条件を設定してバックアップ／リストア処理用の利用権情報を設定発行してもよい。

【0178】

[8. リコメンドファイルによるコンテンツの二次配信]

次に、正規にコンテンツを購入したクライアントが、購入コンテンツを他のクライアントに提供するいわゆるコンテンツ二次配信を実行し、コンテンツ利用権をライセンスサーバから新たに配布することで、二次配信コンテンツを受領したクライアントにおいても正当なコンテンツ利用権を有することを条件としてコンテンツ利用を可能とし、さらに、コンテンツサーバからのコンテンツ配信負荷の軽減を実現した構成について説明する。

【0179】

前述したように、コンテンツを再生利用するクライアントは、コンテンツを利用するためには、コンテンツサーバから暗号化されたコンテンツを受け取るとともに、ライセンスサーバから、ライセンス情報、すなわちサービスデータと、コンテンツに対応する利用権情報を受領することが必要となる。

【0180】

ライセンス情報、すなわちサービスデータおよび利用権情報は、データ容量の小さいデータであるため、インターネット等の通信網を介した送受信が頻繁に行われたとしてもトラフィックの上昇も少なく、多大な配信時間がかかるといった問題は発生しない。しかし、一方、コンテンツは、音楽データ、画像データ、プログラム等様々であり、そのデータ容量も大きなものとなる。このような大容量のコンテンツを特定のコンテンツサーバから多くのクライアントに送信する場合には、送信時間が長くなり、コンテンツサーバの負担、ネットワークトラフィックの上昇等、様々な問題を発生させる。また、通信中の通信エラーによるコンテンツ配信エラーのトラブルも発生しかねない。

【0181】

以下では、すでに正規なコンテンツを購入したクライアントの保有するコンテンツを他のクライアントに提供、すなわち二次配信を実行し、二次配信によるコンテンツの提供を受けたクライアントが、そのコンテンツのライセンス情報をライセンスサーバから受領することで、コンテンツサーバのクライアントに対するコンテンツ送信の負荷を減少させたシステムについて説明する。

【0182】

図28にコンテンツを正規に受領したクライアントが他のクライアントに提供するコンテンツファイルを生成する処理手順を説明したフローを示す。なお、他のクライアントに提供するコンテンツを含むデータファイルをリコメンドファイルと呼ぶ。リコメンドファイルには、暗号化されたコンテンツを含むコンテンツファイル、および必要に応じてそのコンテンツの説明ファイル(例えばHTMLファイル)が含まれる。

【0183】

図28の処理フローについて説明する。図28の処理を実行するクライアントは、前述したコンテンツ購入処理を実行し、正規にコンテンツを購入したクライアント、

あるいは、リコメンドファイルを他のクライアントから受領し、その後の手続きにおいて正規なライセンスを取得したクライアントである。図28の処理は、クライアントアプリケーション（図1のクライアントアプリケーション12）の1つの実行プログラムとしてクライアントシステムとしての情報処理装置の制御手段（CPU等）による制御の下に実行される。ステップS801において、クライアントは、自己のクライアント装置のディスプレイにリコメンドファイル作成画面を表示する。

【0184】

リコメンドファイル作成画面例を図29に示す。クライアントが正規購入し、再生可能なコンテンツリスト651が中央に表示され、リコメンドファイルを生成する場合は、このコンテンツリスト651からコンテンツを選択（ステップS802）し、右側のリスト654にタイトル等を表示させる。コンテンツリスト651とリスト654間の移動処理は、移動スイッチ652、653の操作によって実行される。

【0185】

リコメンドファイル生成対象コンテンツが選択されると、ステップS803において、リコメンドファイル作成ボタン655が押下される。リコメンドファイル作成ボタン655が押下されると、ステップS804において、リコメンドファイル内にコンテンツファイルに併せて説明ファイル、例えばHTMLによって記述された説明ファイルを生成格納するか否かを選択する。これはユーザが任意に選択可能である。

【0186】

リコメンドファイルには、図30（a）に示すように、暗号化コンテンツを含むコンテンツファイル721とコンテンツ説明ファイル722とを組み合わせたリコメンドファイル720構成と、図30（b）に示すように、暗号化コンテンツを含むコンテンツファイル721のみからなるリコメンドファイル730構成との2つの態様があり、クライアントはその態様を自由に選択可能となる。

【0187】

ステップS804において、コンテンツ説明用ファイルの作成をしないと選択した場合は、図30（b）に示すコンテンツファイル721のみからなるリコメンドファイル730が生成される。

【0188】

コンテンツファイルの構成を図31に示す。コンテンツファイル（MQTファイル）721には、暗号化コンテンツと、コンテンツ付加情報としてのメタ情報、さらにコンテンツ購入可能なショップを示すショップサーバURL、コンテンツ識別子としてのコンテンツID（CID）が含まれる。

【0189】

なお、コンテンツファイルに格納される暗号化コンテン

ツは、コンテンツキーKcにより暗号化されたコンテンツであり、コンテンツキーKcは、有効化キーブロック（EKB）配信ツリー構成を適用して提供される有効化キーブロック（EKB）の復号により取得可能なキーの適用によってのみ取得可能なキーである。

【0190】

一方、ステップS804において、コンテンツ説明用ファイル作成を選択した場合は、ステップS806に進み、コンテンツ説明ファイル（HTMLファイル）生成用の説明データ（メタデータ）をコンテンツ管理テーブルから取得する。コンテンツに対応するコンテンツ説明データは、上述したように暗号化コンテンツとともに、コンテンツファイル内にも格納されているが、正規にコンテンツ利用権を取得したクライアントは、コンテンツファイルから取り出したコンテンツ対応のメタデータをコンテンツ管理データとして、別ファイルに格納管理しており、リコメンドファイルにおいて生成される説明ファイル用のメタデータは、このコンテンツ管理データから抽出される。

【0191】

ステップS807において、コンテンツ管理データから抽出したメタデータを、クライアントアプリケーションに設定されたテンプレートHTMLファイルに貼り付ける処理を実行し、コンテンツ対応の説明用HTMLファイルを生成し、ステップS808において、コンテンツファイルと説明用HWMMLファイルからなるリコメンドファイルを生成する。

【0192】

コンテンツ説明用データとしてのHTMLファイルの表示構成例を図32に示す。図32に示す例は、コンテンツが音楽データの場合の例である。説明用ファイルは、図32に示すように、音楽コンテンツの楽曲タイトル、アーティスト、発売元等の情報リスト、さらに、各種の操作、処理に関する説明が記述されている。リコメンドファイルを他のクライアントから受領したクライアントは、まずこの説明ファイルをオープンすることになる。

【0193】

リコメンドファイルに格納されたコンテンツは暗号化されたコンテンツであり、正規なライセンス情報、すなわちサービスデータとコンテンツ対応の利用権情報を取得していない場合には再生することはできない。従って、リコメンドファイルを受領したクライアントがリコメンドファイルに格納されたコンテンツを利用する場合には、ライセンス情報を取得する手続きを実行することになる。

【0194】

このライセンス情報取得処理について、図33、図34の処理フローを参照して説明する。リコメンドファイルを受領したクライアントは、図32に示す説明用ファイル（HTMLファイル）をオープンし、試聴、購入コン

処理については省略してあるが、サービスデータを保有していないクライアントがリコメンドファイルを受領した場合には、ライセンスサーバに対するアクセスを実行して登録処理を行ない、サービスデータを取得することが必要となる。この登録処理手続きは、先に図13、図16を参照して説明した処理に対応する処理となる。

【0206】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0207】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【0208】

例えば、プログラムは記憶媒体としてのハードディスクやROM(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0209】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体にインストールすることができる。

【0210】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【0211】

【発明の効果】

以上、説明したように、本発明の構成によれば、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報(Default Usage Right)を取得し、コンテンツの購入処理を伴わない試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生が許可され、ユーザは、コンテンツの購入を実行することなく、コンテンツの試聴再生が可能となる。また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

【0212】

さらに、本発明の構成によれば、コンテンツの購入処理を伴わない試聴処理においても、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB[EKB(H)]と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB[EKB(S)]に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴処理においても再生権限を限定した範囲として設定可能となる。

【図面の簡単な説明】

【図1】本発明を適用したコンテンツ提供システムの概要を示す図である。

【図2】クライアント、および各サーバ、管理システムの構成例を示す図である。

【図3】各種キー、データの暗号化処理、配布処理について説明するツリー構成図である。

【図4】各種キー、データの配布に使用される有効化キーブロック(EKB)の例を示す図である。

【図5】コンテンツキーの有効化キーブロック(EKB)を使用した配布例と復号処理例を示す図である。

【図6】有効化キーブロック(EKB)のフォーマット例を示す図である。

【図7】有効化キーブロック(EKB)のタグの構成を説明する図である。

【図8】ツリー構成におけるカテゴリ分割を説明する図である。

【図9】ツリー構成におけるカテゴリ分割を説明する図である。

【図10】ツリー構成におけるカテゴリ分割の具体例を説明する図である。

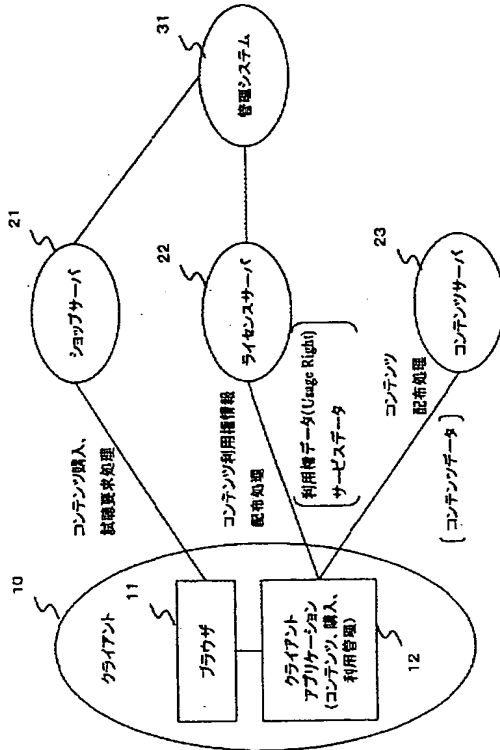
【図11】コンテンツ購入、または試聴処理における各エンティティ間の実行処理シーケンス(その1)を示す図である。

【図12】管理システムにおいて実行するトランザクションID生成、発行処理手順を示すフロー図である。

47

- 401 サービスデータ
- 402 暗号化コンテンツファイル
- 403 利用権情報
- 411 EKB (H)
- 601 リストア処理要求ファイル
- 651 コンテンツリスト
- 652, 653 スイッチ

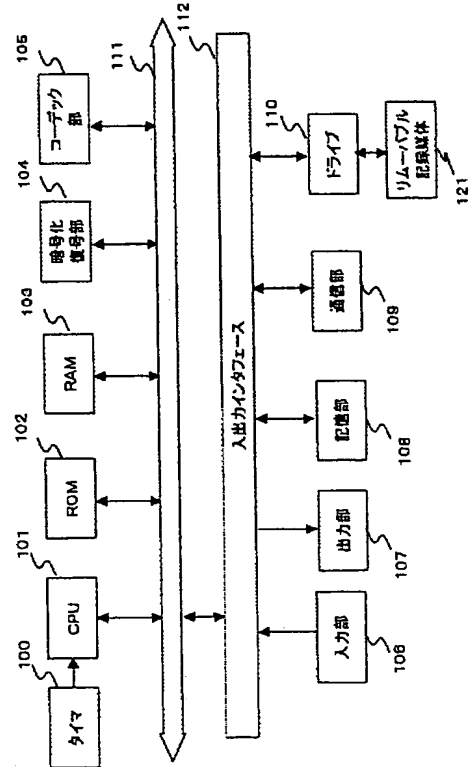
【図1】



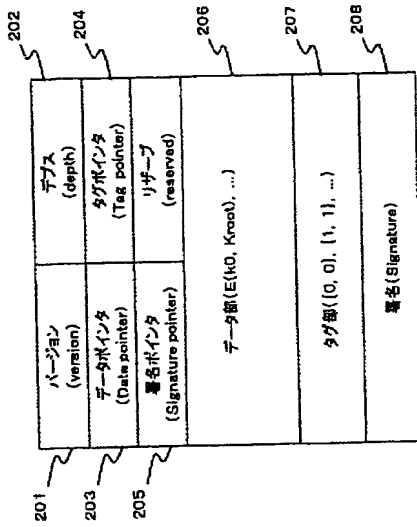
48

- 653 リコメンドファイル作成ボタン
- 654 リスト
- 720, 730 リコメンドファイル
- 721 コンテンツファイル
- 722 コンテンツ説明ファイル
- 731 試聴、購入コンテンツ配信サイトボタン

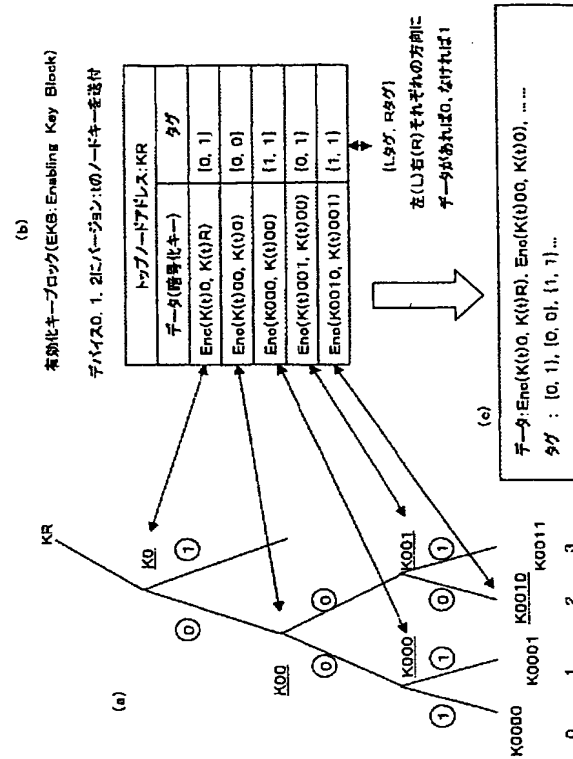
【図2】



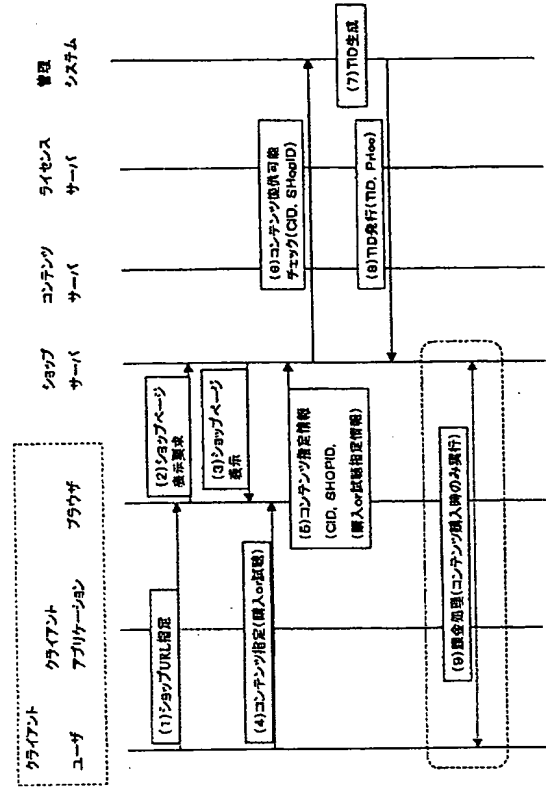
【図6】



【図7】

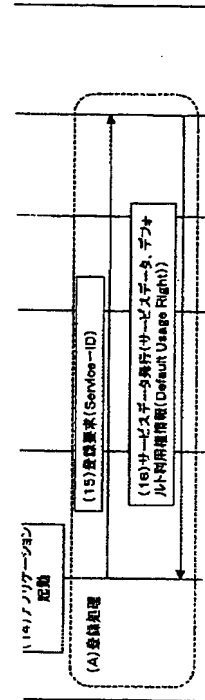
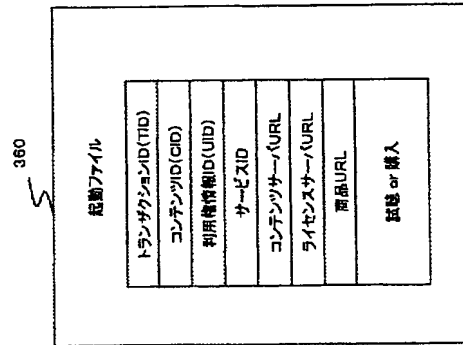
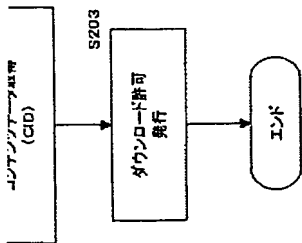


【图 1 1】

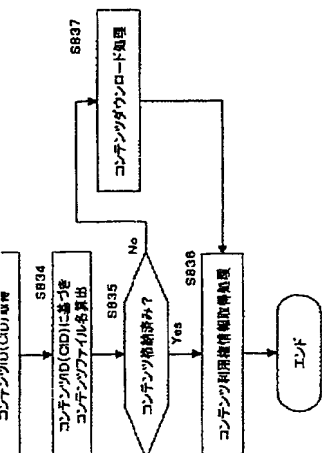


14】

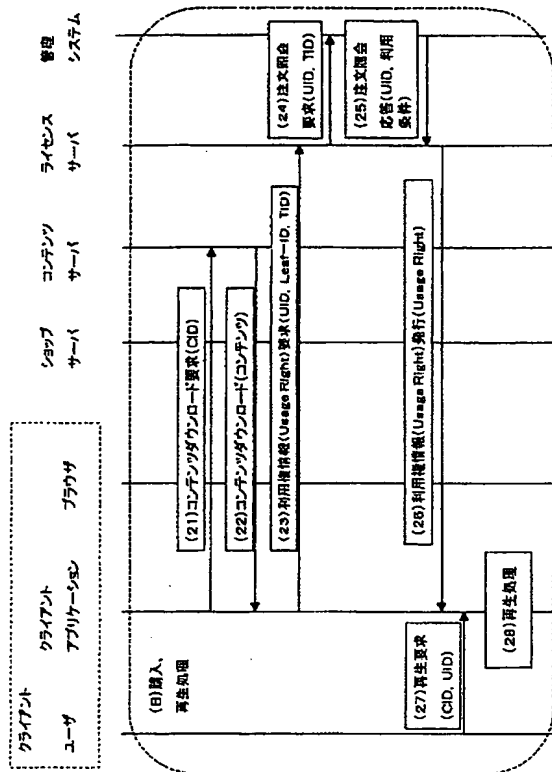
【図15】



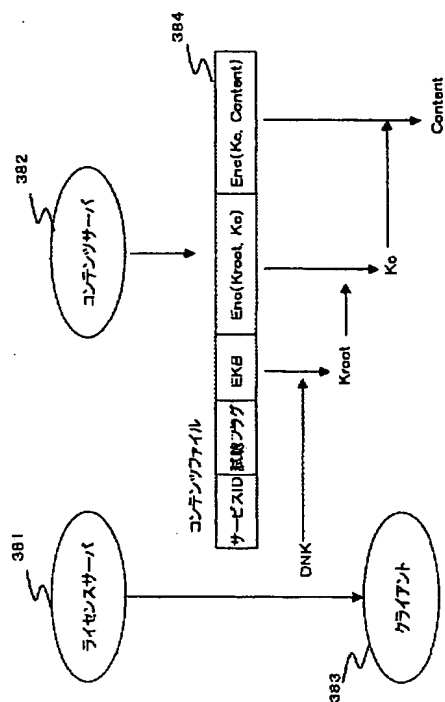
【図34】



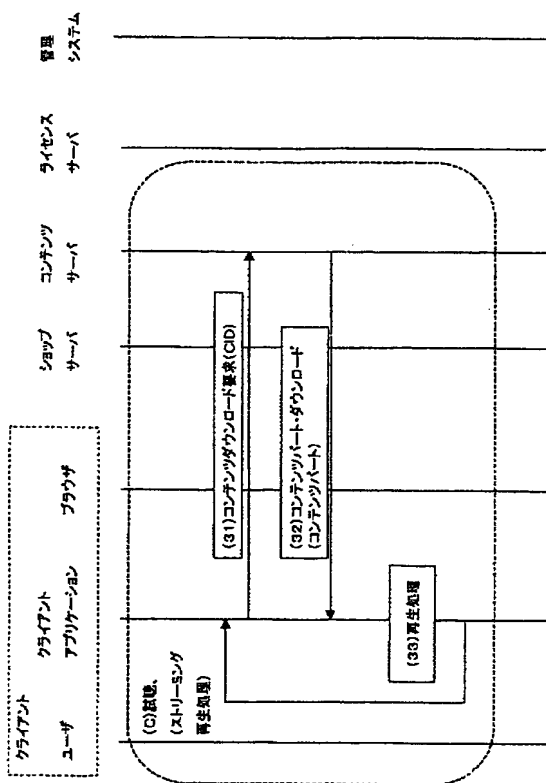
【図18】



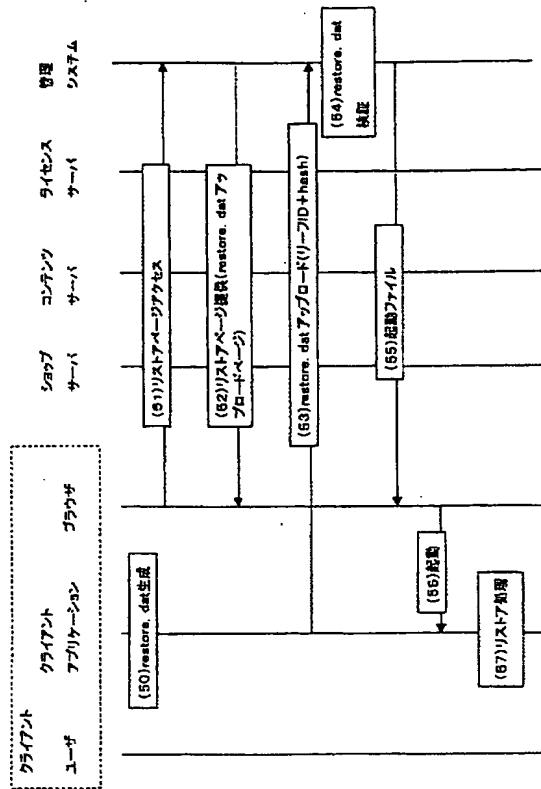
【図19】



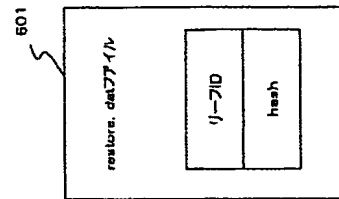
【图 2 1】



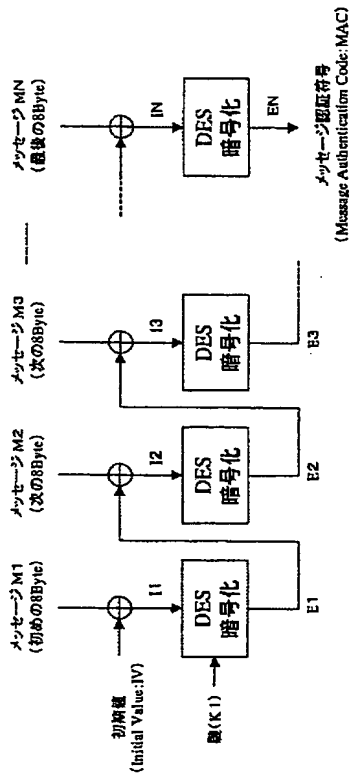
【図23】



【図24】

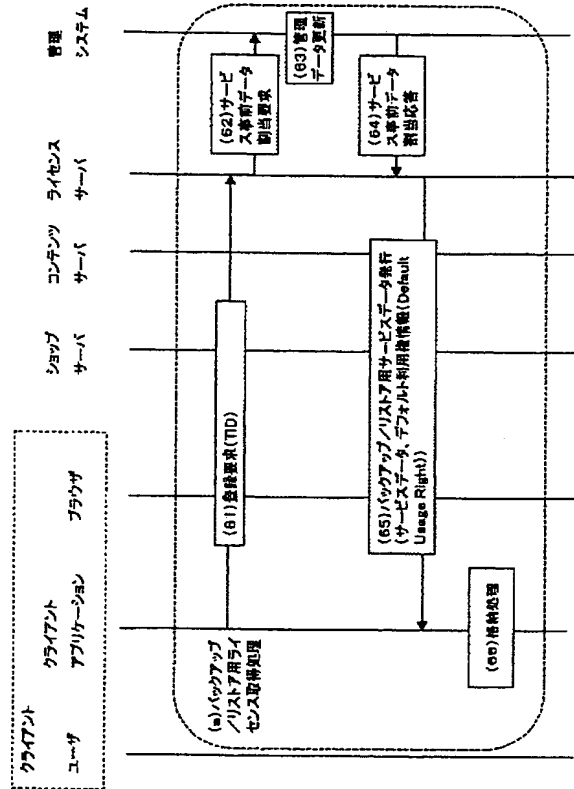


【図25】

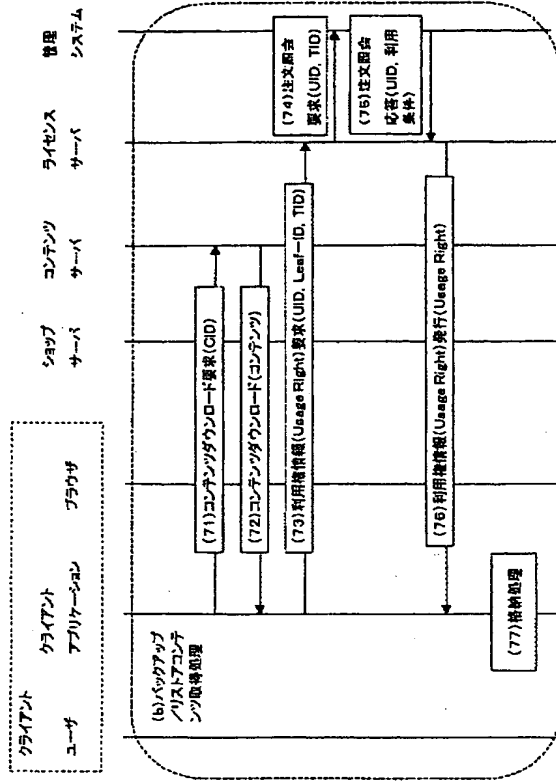


⊕ : 排他的論理和処理 (8バイト単位)

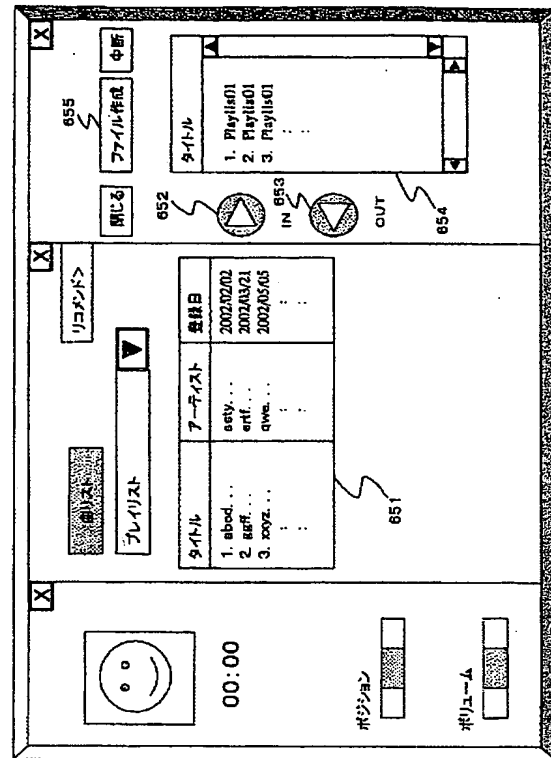
【図26】



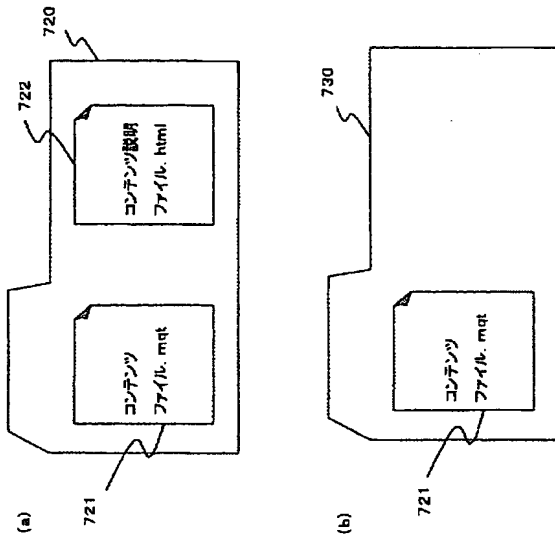
【図27】



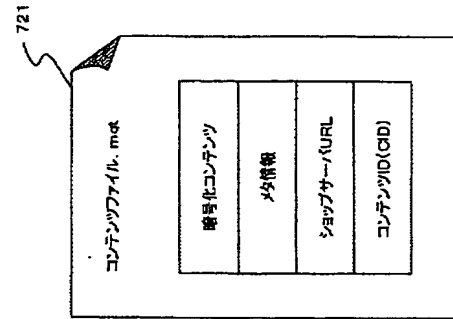
【図29】



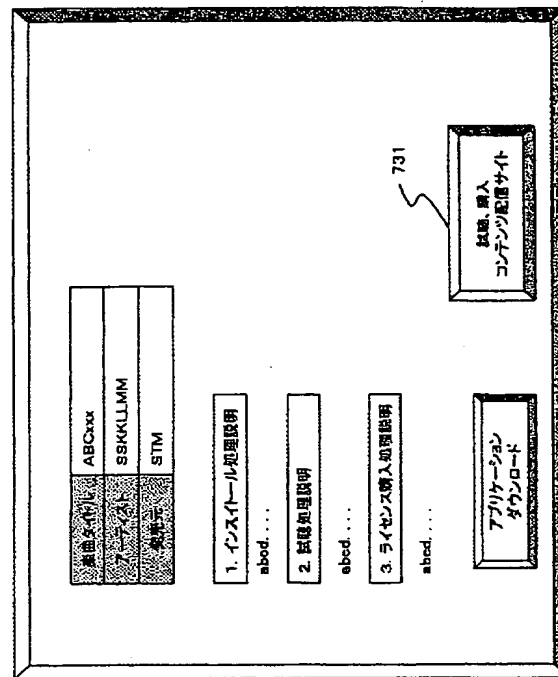
【図30】



【図31】



【図32】



フロントページの続き

(51) Int. Cl.⁷

F I

テーマコード (参考)

G O 6 F 17/60 Z E C
H O 4 N 7/173 6 4 0 A
H O 4 L 9/00 6 0 1 B

Fターム(参考) 5B017 AA03 BA09 CA16

5C064 BA07 BB02 BC06 BC16 BC17 BC20 BC22 BD02 BD07 BD09

5J104 AA16 EA15 PA07 PA10

THIS PAGE BLANK (USPTO)

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 524 604 A1

(12)

EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
20.04.2005 Bulletin 2005/16(51) Int Cl.7: **G06F 12/14**, H04L 9/08,
G06F 17/60

(21) Application number: 03738574.7

(86) International application number:
PCT/JP2003/008267

(22) Date of filing: 30.06.2003

(87) International publication number:
WO 2004/010307 (29.01.2004 Gazette 2004/05)(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT SE SI SK TR• KURIYA, Shinobu, c/o SONY CORPORATION
Tokyo 141-0001 (JP)

(30) Priority: 23.07.2002 JP 2002213700

(71) Applicant: Sony Corporation
Tokyo 141-0001 (JP)(74) Representative: Horner, David Richard et al
IBM United Kingdom Limited,
Intellectual Property Department,
Hursley Park
Winchester, Hampshire SO21 2JN (GB)(72) Inventors:
• KITAYA, Yoshimichi, c/o SONY CORPORATION
Tokyo 141-0001 (JP)(54) **INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND
COMPUTER PROGRAM**

(57) To provide an apparatus and method for realizing an improved content preview process in a content using mechanism based on content usage-right information. A client obtains default usage-right information (Default Usage Right) when it is registered to a license server, and determines, based on the default usage-

right information, whether or not the content can be played back in a content preview process without purchasing the content. The client which is permitted to preview the content is limited to a client which has been registered to the license server to obtain the default usage-right information. This prevents preview-data from being randomly distributed.

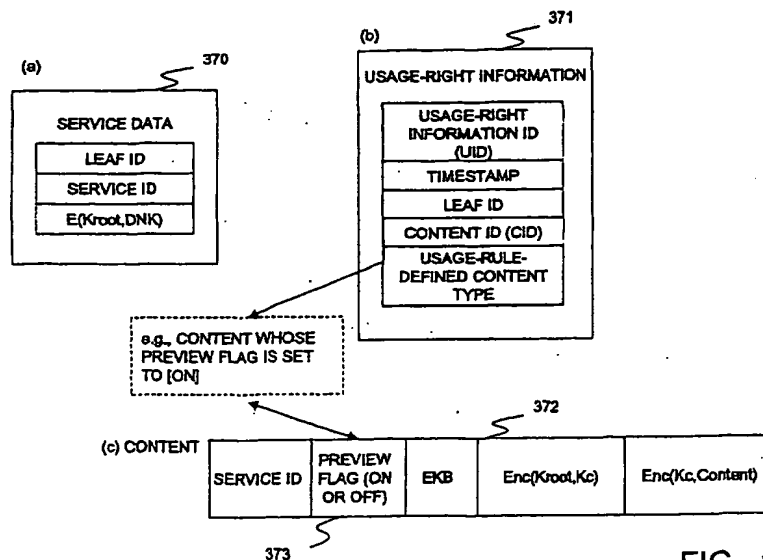


FIG. 17

EP 1 524 604 A1

Description

Technical Field

[0001] The present invention relates to an information processing apparatus, an information processing method, and a computer program. In particular, the present invention relates to an information processing apparatus, an information processing method, and a computer program which realize content usage-right checking when content is used, such as when content is played back, and which allow for audio and visual preview of the content so as to provide users with flexible content use experiences.

Background Art

[0002] Recently, distribution of various software data, such as music data, game programs, image data (such data is hereinafter referred to as content), via networks, such as the Internet, or distributable storage media, such as memory cards, HDs, DVDs, and CDs, has become popular. The distributed content is played back once it is stored in an internal storage unit, e.g., an HD, of a user's PC (Personal Computer), recording/playback device, playback-only device, or game devices, a card-type storage device having a flash memory, a CD, a DVD, etc.

[0003] An information device, such as a recording/playback device, a game device, and a PC, has an interface through which content is received over a network or an interface through which the device accesses a memory card, an HD, a DVD, a CD, etc., a controller necessary for playback of the content, a RAM used as a memory area for a program and data, a ROM, and so on.

[0004] Various content, such as music data, image data, or a program, is invoked by a user instruction from an information device itself, such as a recording/playback device used as a playback device, a game device, or a PC, or a user instruction using a connected input unit so as to be retrieved from, for example, a built-in or removable storage medium. The content is played back by the information device or via a display, speaker, etc., connected thereto.

[0005] In general, authors or sellers of many types of software content, such as game programs, music data, and image data, hold the distribution rights thereof or the like. In distributing the content, therefore, security measures are usually taken against unauthorized duplication by providing certain usage limitations, that is, by permitting only the authorized user to use the software.

[0006] A mechanism in which content and a usage right for using the content are managed independently and are offered to a user has been proposed. In this mechanism, for example, the user must obtain encrypted content and purchase usage-right data thereof to obtain a key (content key) for decoding the encrypted con-

tent based on key data or the like, which can be obtained from the usage-right data, in order to use the content.

[0007] The usage-right data contains setting information indicating the manner that the user can use the content, so that the user can use the content within the range permitted by the permission information. Such a system has been proposed.

Disclosure of Invention

[0008] Accordingly, in the system in which content and a content usage right are independently managed and are offered to users, the usage-right data must be checked when the content is used, for example, when music data or image data is played back, distributed, or downloaded.

[0009] In this mechanism, if it is determined that a user is not authorized to use the content as a result of the usage-right checking, the content cannot be played back, distributed, or downloaded.

[0010] However, actually, there exists a demand for audio or visual preview of a portion of the content, before the content is purchased, in order to demonstrate the content before purchasing. In such a case, because it is determined in a standard content usage-right checking process that the usage right is absent, playback or the like of the content will be rejected.

[0011] In order to overcome such a drawback, it is conceivable that free sample data, which does not consider usage rights, is distributed to users. However, most content has copyright and distribution rights maintained by its author and distributor, respectively, and therefore it is undesirable that the content, even a portion of the content, be randomly distributed and be copied from one user to another without authorization.

[0012] The present invention has been made in view of such a background. It is an object of the present invention to provide an information processing apparatus, an information processing method, and a computer program which allow a user who purchases authorized content to use the authorized content based on usage rights and to audibly or visually preview the content without purchasing the content.

[0013] It is another object of the present invention to provide an information processing apparatus, an information processing method, and a computer program which can prevent random secondary distribution of audio or visual preview-data.

[0014] In a first aspect, the present invention provides an information processing apparatus for controlling decoding and using of encrypted content, the information processing apparatus including:

control means for controlling content use based on usage-right information corresponding to the content according to an instruction to use the content; and
recording means for recording default usage-right

information, the default usage-right information being recorded in manufacturing or being obtained at a service registration time,

wherein the control means permits the content to be decoded and used based on the description of the default usage-right information when the content includes information indicating association with the default usage-right information.

[0015] In an embodiment of the information processing apparatus of the present invention, the content which is permitted for use based on the default usage-right information is provided for the purpose of sampling, and the control means determines whether or not the content includes a flag indicating sample content, and permits playback of the content according to a determination result.

[0016] In another embodiment of the information processing apparatus of the present invention, the information processing apparatus further includes sending means for sending a service registration request, and receiving means for receiving the default usage-right information sent from a license server in response to the registration request.

[0017] In another embodiment of the information processing apparatus of the present invention, the receiving means further receives key information necessary for decoding the content.

[0018] In a second aspect, the present invention provides an information processing apparatus for issuing a usage right having usage rules of encrypted content, the information processing apparatus including:

receiving means for receiving a registration request; and

sending means for sending key information and default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content.

[0019] In an embodiment of the information processing apparatus of the present invention, the content which is permitted for use based on the default usage-right information is provided for the purpose of sampling, and the default usage-right information includes a description indicating that playback of the content is permitted when the content includes a flag indicating sample content.

[0020] In a third aspect, the present invention provides an information processing method for controlling decoding and using of encrypted content, the information processing method including a control step of controlling content use based on usage-right information corresponding to the content according to an instruction to use the content,

wherein the control step includes:

a step of determining whether or not the content in-

cludes information indicating association with default usage-right information recorded in manufacturing or default usage-right information obtained at a service registration time; and

a step of permitting the content to be decoded and used based on the description of the default usage-right information when the content includes the information indicating association with the default usage-right information.

[0021] In an embodiment of the information processing method of the present invention, the content which is permitted for use based on the default usage-right information is provided for the purpose of sampling, and the control step further includes a step of determining whether or not the content includes a flag indicating sample content, and permitting playback of the content according to a determination result.

[0022] In another embodiment of the information processing method of the present invention, the information processing method further includes a sending step of sending a service registration request, and a receiving step of receiving the default usage-right information sent from a license server in response to the registration request.

[0023] In another embodiment of the information processing method of the present invention, the information processing method further includes a step of receiving key information necessary for decoding the content.

[0024] In a fourth aspect, the present invention provides an information processing method for issuing a usage right having usage rules of encrypted content, the information processing method including:

a receiving step of receiving a registration request; and

a sending step of sending key information and default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content.

[0025] In an embodiment of the information processing method of the present invention, the content which is permitted for use based on the default usage-right information is provided for the purpose of sampling, and the default usage-right information includes a description indicating that playback of the content is permitted when the content includes a flag indicating sample content.

[0026] In a fifth aspect, the present invention provides a computer program for performing an information process for controlling decoding and using of encrypted content, the computer program including a control step of controlling content use based on usage-right information corresponding to the content according to an instruction to use the content,

wherein the control step includes:

a step of determining whether or not the content includes information indicating association with default usage-right information recorded in manufacturing or default usage-right information obtained at a service registration time; and
 a step of permitting the content to be decoded and used based on the description of the default usage-right information when the content includes the information indicating association with the default usage-right information.

[0027] In an embodiment of the computer program of the present invention, the content which is permitted for use based on the default usage-right information is provide for the purpose of sampling, and the control step further includes a step of determining whether or not the content includes a flag indicating sample content, and permitting playback of the content according to a determination result.

[0028] In another embodiment of the computer program of the present invention, the computer program further includes a sending step of sending a service registration request, and a receiving step of receiving the default usage-right information sent from a license server in response to the registration request.

[0029] In another embodiment of the computer program of the present invention, the computer program further includes a step of receiving key information necessary for decoding the content.

[0030] In a sixth aspect, the present invention provides a computer program for performing an information process for issuing a usage right having usage rules of encrypted content, the computer program including:

a receiving step of receiving a registration request;
 a sending step of sending key information and default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content.

[0031] In an embodiment of the computer program of the present invention, the content which is permitted for use based on the default usage-right information is provided for the purpose of sampling, and the default usage-right information includes a description indicating that playback of the content is permitted when the content includes a flag indicating sample content.

[0032] In a seventh aspect, the present invention provides a content usage management system including a content using apparatus for decoding and using encrypted content, and a usage-right issuing apparatus for issuing a usage right having usage rules of the encrypted content, wherein the content using apparatus includes:

sending means for sending a service registration request; and
 receiving means for receiving default usage-right

information sent from a license server in response to the registration request, and
 the usage-right issuing apparatus includes:
 receiving means for receiving the registration request; and
 sending means for sending key information and the default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content.

[0033] In an eighth aspect, the present invention provides a content usage managing method for a content usage management system including a content using apparatus for decoding and using encrypted content, and a usage-right issuing apparatus for issuing a usage right having usage rules of the encrypted content, the content usage managing method including:

a registration-request sending step of sending a service registration request from the content using apparatus to the usage-right issuing apparatus;
 a data sending step of, in the usage-right issuing apparatus, receiving the registration request and sending key information and default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content; and
 a receiving step of, in the content using apparatus, receiving the default usage-right information.

[0034] According to the structure of the present invention, a client obtains default usage-right information (Default Usage Right) when it is registered to a license server, and is permitted to play back the content based on the default usage-right information in a content preview process without purchasing the content. Therefore, the user is able to preview and play back the content without purchasing the content. The client which is permitted to preview the content is limited to a client which has been registered to the license server to obtain the default usage-right information. This prevents preview-data from being randomly distributed.

[0035] According to the structure of the present invention, furthermore, also in the content preview process without purchasing the content, only the user having authorized DNKs for a hardware EKB [EKB(H)] serving as an EKB corresponding to a category tree established for hardware devices, which are content-using devices, and a service EKB [EKB(S)] serving as an EKB corresponding to a category tree established for content-using services can play back the content and preview the content with limited playback control.

[0036] The computer program of the present invention is a computer program which can be offered in the computer-readable form to, for example, a general-purpose computer system capable of executing various program code by means of storage media or communication media, for example, storage media such as CDs,

FDs, and MOs, or communication media such as a network. Such a computer-readable program is offered, so that the process according to the program can be performed on a computer system.

[0037] Other objects, features, and advantages of the present invention will become apparent from the following detailed description of an embodiment of the present invention taken in conjunction with the appended drawings. As used herein, the term system is a logical set of a plurality of apparatuses, and these apparatuses are not necessarily housed in the same case.

Brief Description of the Drawings

[0038]

Fig. 1 is a schematic diagram showing the overview of a content providing system according to the present invention.

Fig. 2 is a diagram showing an example structure of each of a client, servers, and a management system.

Fig. 3 is a tree structural view showing a process for encrypting various keys and data and a process for delivering the encrypted keys and data.

Fig. 4 is an illustration of an example enabling key block (EKB) used for delivery of the various keys and data.

Fig. 5 is an illustration of an example delivery and decoding process of a content key using an enabling key block (EKB).

Fig. 6 is a view showing an example format of an enabling key block (EKB).

Fig. 7 is an illustration of the tag structure of the enabling key block (EKB).

Fig. 8 is an illustration of category division in the tree structure.

Fig. 9 is an illustration of category division in the tree structure.

Fig. 10 is an illustration of a specific example of category-based division in the tree structure.

Fig. 11 is a chart showing a sequence (part 1) of operation steps performed between entities in a content purchase or preview process.

Fig. 12 is a flow diagram showing a procedure for generating and issuing a transaction ID performed in a management system.

Fig. 13 is a chart showing a sequence (part 2) of operation steps performed between the entities in the content purchase or preview process.

Fig. 14 is a flow diagram showing a download permission procedure performed in the management system.

Fig. 15 is a view showing an example data structure of a start-up file.

Fig. 16 is a flow diagram showing an application executing procedure based on the start-up file performed by a client.

Fig. 17 is a view showing an example data structure of service data and usage-right information.

Fig. 18 is a chart showing a sequence of operation steps performed between the entities in the content purchase process.

Fig. 19 is a diagram showing the overview of a content playback process.

Fig. 20 is a diagram showing an example process for decoding and using content using an enabling key block (EKB).

Fig. 21 is a chart showing a sequence of operation steps performed between the entities in the content preview process.

Fig. 22 is a flowchart showing the overview of a preview-content playback process.

Fig. 23 is a chart showing a sequence (part 1) of operation steps performed between entities in a license or content backup/restoration process.

Fig. 24 is a view showing an example structure of a restoration request file [restore.dat].

Fig. 25 is a view showing a MAC generation mechanism.

Fig. 26 is a chart showing a sequence (part 2) of operation steps performed between the entities in the license or content backup/restoration process.

Fig. 27 is a chart showing a sequence (part 3) of operation steps performed between the entities in the license or content backup/restoration process.

Fig. 28 is a flowchart showing a recommendation file generation process.

Fig. 29 is an illustration of a recommendation file generation view.

Fig. 30 is a view showing an example structure of a recommendation file.

Fig. 31 is a view showing an example structure of a content file contained in the recommendation file.

Fig. 32 is a view showing a display example of a content description file contained in the recommendation file.

Fig. 33 is a flowchart (part 1) for a license information obtaining process of a client which has received the recommendation file.

Fig. 34 is a flowchart (part 2) for the license information obtaining process of the client which has received the recommendation file.

Best Mode for Carrying Out the Invention

[0039] The structure of the present invention is described in detail hereinbelow. The description is made in the context of items listed below:

1. Content Providing System Overview
2. Regarding Tree Structure as Key Distribution Mechanism
3. EKB-based Key Distribution
4. EKB Format
5. Category Classification of Tree

- 6. Content Purchase and Preview Process
- 7. Backup/Restoration Process
- 8. Secondary Distribution of Content Based on Recommendation File

[1. Content Providing System Overview]

[0040] Fig. 1 is a diagram showing the overview of a content providing system in accordance with the present invention. A client 10 which uses content is an information processing apparatus serving as a device capable of using, or playing back, the content, such as a PC or a PDA. The client 10 has a browser 11 and a client application 12, which are implemented in software, and a controller, such as a CPU, executes programs of the browser 11, the client application 12, and the like.

[0041] The client application 12 is an application for performing a content purchase and preview process on the client, a process for obtaining license information including service data and content usage-right information, as described below, a backup/restoration process of content and license information, a content usage-right checking process, a content playback management process, a process for generating a recommendation file serving as a content file for secondary distribution, and so on. The client application 12 is stored as a processing program in the client information processing apparatus, as described in detail below. As used herein, "preview" includes not only audible preview of audio data but also visual preview of image data.

[0042] The client 10 is connected to a shop server 21, a license server 22, and a content server 23 via a communication network, such as the Internet. The content server 23 sends content to the client 10. The license server 22 sends usage-right information of the content to be used by the client to the client 10. The shop server 21 functions as a contact accessed by the client 10 to purchase the content. The shop server 21 provides the content which can be purchased or previewed via the browser, and receives a purchase or preview request from the client. The shop server 21 also performs a billing operation for the purchased content, if necessary.

[0043] The shop server 21 and the license server 22 are also connected with a management system 31. The management system 31 issues a transaction ID (TID) serving as permission information in response to a content request from the client 10 received by the shop server 21, and also issues content download permission information. The management system 31 further authorizes the license server 22 to issue usage-right data (Usage Right) serving as content usage-right information. The details of these processes are described below.

[0044] The client 10 obtains the usage right from the license server 22 and the content from the content server 23 under the control of the client application 12. The client 10 starts the browser 11 under the control of the client application 12 to perform a preview and payment process for the information provided by the shop server

21.

[0045] Although only one client, shop server, license server, and content server are shown in Fig. 1, multiple clients, shop servers, license servers, and content servers are connected across a communication network, such as the Internet. Each client is free to access various shop servers to select desired items from the content provided by the shop servers to obtain the content from a content server which stores the selected content. The client further selects a license server which issues the usage right of the obtained content to obtain the usage right from the selected license server.

[0046] The content is sent as encrypted content to the client 10 from the content server 23. The license server 22 also sends the content usage-right information corresponding to the content to the client 10. The usage-right information is verified by the client application 12 of the client 10, and the encrypted content is decoded when it is determined the usage right is present.

[0047] The client 10 has key information for allowing content use based on the content usage right, that is, key data including an enabling key block (EKB), a device node key (DNK), and so forth. The enabling key block (EKB) and the device node key (DNK) are key data for obtaining an encryption key necessary for content use, which allows only the user device having the authorized content usage right to decode and use the encrypted content. The EKB and the DNK are described below.

[0048] The content server 23 encrypts content, and sends the encrypted content to the client 10. The license server 22 generates usage-right information (Usage Right) based on content usage rules and conditions, and sends the generated usage right to a user device 30. The license server 22 further generates service data based on the device node key (DNK) and enabling key block (EKB) provided by the management system 31, and sends the generated service data to the client 10. The service data includes an enabling key block (EKB) having a service device node key (SDNK) necessary for decoding the encrypted content.

[0049] The content usage rules include a requirement on a limited use period, a limited time the content can be copied, a limited number of portable media (PM) which can concurrently use the content (this number corresponds to the number of so-called check-outs), and so on. The portable media (PM) are storage media for use in portable devices, such as a flash memory, of a mini HD, an optical disk, a magneto-optical disk, and an MD (Mini Disk).

[0050] An example structure of an information processing apparatus which can function as each of the client 10, the shop server 21, the license server 22, the content server 23, and the management system 31 is shown in Fig. 2. Each system is realized by storing a process program corresponding to each operation in a system having a CPU, such as a PC or a server.

[0051] An example structure of each system will be described with reference to Fig. 2. A CPU (Central

Processing Unit) 101 executes various operations according to various programs stored in a ROM (Read Only Memory) 102 or a program stored in a storage unit 108 and loaded to a RAM (Random Access Memory) 103. A timer 100 performs a clock operation, and supplies clock information to the CPU 101.

[0052] The ROM (Read Only Memory) 102 stores a program used by the CPU 101, calculation parameters, fixed data, and so on. The RAM (Random Access Memory) 103 stores a program used for execution of the CPU 101, parameters which appropriately vary depending upon the executed program, and so on. These components are connected with each other via a bus 111, such as a CPU bus.

[0053] An encryption/decryption unit 104 performs a content encryption and decryption process, an encryption process using, for example, a DES (Data Encryption Standard) encryption algorithm, which is applied to a device node key (DNK) and an enabling key block (EKB), a MAC generation and verification process, etc. The encryption/decryption unit 104 also performs various encryption processes, such as authentication for transmission and reception of content or license information between this device and another device connected thereto, and session key sharing process.

[0054] A codec unit 105 encodes and decodes data using various techniques, such as ATRAC (Adaptive Transform Acoustic Coding)-3, MPEG, and JPEG. The data to be processed is input via the bus 111, an input/output interface 112 from a removable storage medium 121 via a drive 110 or from a communication unit 109. The processed data is stored in the removable storage medium 121 or is output from the communication unit 109 according to necessity.

[0055] An input unit 106, including a keyboard and a mouse, an output unit 107 including a display, such as a CRT or an LCD, and a speaker, the storage unit 108 such as a hard disk, the communication unit 109 formed of a modem, a terminal adapter, etc., are connected with the input/output interface 112 so as to transmit and receive data over a communication network, such as the Internet.

[2. Regarding Tree Structure as Key Distribution Mechanism]

[0056] A device and key management mechanism using a tree, which is one form of broadcast encryption scheme which enables only a client having an authorized content usage right to use the content will be described.

[0057] In Fig. 3, devices numbered 0 to 15 at the bottom are user devices serving as clients which use the content. Leaves of the hierarchical tree structure shown in Fig. 3 correspond to devices.

[0058] Each of the devices 0 to 15 stores a key set (device node key (DNK)) formed of keys (node keys) assigned to the nodes from the leaf of each device to

the root in the tree shown in Fig. 3 and a leaf key of each leaf in its memory when or after each device is manufactured or shipped. In Fig. 3, K0000 to K1111 at the bottom are leaf keys assigned to the devices 0 to 15, respectively, and keys KR to K111 from the KR (root key) at the top to keys assigned to the nodes in the second layer from the bottom are node keys.

[0059] In the tree structure shown in Fig. 3, for example, the device 0 has a leaf key K0000, and node keys K000, K00, K0, and KR. The device 5 has K0101, K010, K01, K0, and KR. The device 15 has K1111, K111, K11, K1, and KR. In the tree shown in Fig. 3, only 16 devices 0 to 15 are shown, and the tree has a symmetrical structure with four layers; however, the tree may include more devices and may have a different number of layers in different portions of the tree.

[0060] The devices in the tree structure shown in Fig. 3 include various types of devices using various recording media such as a DVD, CD, MD, and flash memory embedded in the devices or removable from the devices. A variety of application services can also co-exist. Such co-existence of different devices and different applications is applied with the hierarchical tree structure shown in Fig. 3, which is a content or key distribution mechanism.

[0061] In a system in which various devices and applications co-exist, for example, the components encircled with a dotted line shown in Fig. 3, that is, the devices 0, 1, 2, and 3, are combined into one group using the same recording medium. For example, the devices belonging to the group encircled with the dotted line are collectively subjected to processing, such that common content is encrypted and is sent to the devices from a provider, a content key shared with the devices is sent to the devices, or content-fee-payment data is encrypted and is output to a provider, a settlement organization, or the like. An organization which transmits and receives data to and from the devices, such as a content server, a license server, or a shop server, sends the data to the portion encircled with the dotted line shown in Fig. 3, or a group of the devices 0, 1, 2, and 3, at the same time. The tree shown in Fig. 3 includes a plurality of groups. An organization which transmits and receives data to and from the devices, such as a content server, a license server, or a shop server, functions as message-data delivery means.

[0062] The node keys and the leaf keys may be managed together by a single management system having a key management center function, or may be managed group-by-group by the message-data delivery means, such as a provider or settlement organization, which transmits and receives various data to and from each group. The node keys and the leaf keys are renewed by a management system having a key management center function, a provider, a settlement organization, or the like, for example, if the keys are intercepted.

[0063] In the tree structure, as is apparent from Fig. 3, each of the three devices 0, 1, 2, and 3 belonging to

the group has a device node key (DNK), i.e., a device node key (DNK) containing the shared keys K00, K0, and KR. This node key sharing mechanism allows, for example, a common key to be sent to only the devices 0, 1, 2, and 3. For example, the shared node key K00 is a common key shared by the devices 0, 1, 2, and 3. Distribution of a value $\text{Enc}(K00, K_{\text{new}})$ formed by encrypting a new key K_{new} using the node key K00 to the devices 0, 1, 2, and 3 via a network or by means of a recording medium having the value allows only the devices 0, 1, 2, and 3 to use their shared node key K00 to decode the encrypted value $\text{Enc}(K00, K_{\text{new}})$ to obtain the new key K_{new} . $\text{Enc}(K_a, K_b)$ represents data formed by encrypting K_b using K_a .

[0064] If it is discovered at a certain time t that the keys K0011, K001, K00, K0, and KR owned by the device 3 have been compromised and revealed by an attacker (hacker), in order to protect data to be exchanged thereafter in the system (a group of the devices 0, 1, 2, and 3), the device 3 must be separated from the system. Therefore, it is necessary to renew the node keys K001, K00, K0, and KR to keys $K(t)001$, $K(t)00$, $K(t)0$, and $K(t)R$, respectively, and to report the renewed keys to the devices 0, 1, and 2. As used herein, $K(t)aaa$ represents a renewed key at generation t of a key Kaaa.

[0065] A process for distributing a renewed key will now be described. Key renewal is carried out by supplying a table formed of block data, called an enabling key block (EKB) shown in, for example, Fig. 4(A), to the devices 0, 1, and 2, for example, over a network or by means of a recording medium having the table stored therein. The enabling key block (EKB) is formed of encrypted keys for distribution of renewed keys to the devices corresponding to the leaves of the tree structure shown in Fig. 3. The enabling key block (EKB) may be referred to as a key renewal block (KRB).

[0066] The enabling key block (EKB) shown in Fig. 4(A) is formed as block data having a data structure which can be updated only by the devices whose node key must be renewed. The example shown in Fig. 4 indicates block data formed for the purpose of distributing renewed node keys at generation t to the devices 0, 1, and 2 in the tree structure shown in Fig. 3. As is apparent from Fig. 3, the device 0 and the device 1 need the renewed node keys $K(t)00$, $K(t)0$, and $K(t)R$, and the device 2 needs the renewed node keys $K(t)001$, $K(t)00$, $K(t)0$, and $K(t)R$.

[0067] As indicated by the EKB shown in Fig. 4(A), the EKB includes a plurality of encrypted keys. The encrypted key at the bottom is $\text{Enc}(K0010, K(t)001)$, which is formed by encrypting the renewed node key $K(t)001$ using the leaf key K0010 of the device 2. The device 2 can use its leaf key to decode the encrypted key to obtain $K(t)001$. The device 2 can further use the $K(t)001$ obtained as a result of decoding to decode the encrypted key $\text{Enc}(K(t)001, K(t)00)$ in the second row from the bottom shown in Fig. 4(A) to obtain the renewed node key $K(t)00$. Likewise, the device 2 can decode the en-

crypt key $\text{Enc}(K(t)00, K(t)0)$ in the second row from the top shown in Fig. 4(A) to obtain the renewed node key $K(t)0$, and can decode the encrypted key $\text{Enc}(K(t)0, K(t)R)$ in the first row from the top shown in Fig. 4(A) to obtain $K(t)R$. On the other hand, the devices K0000 and K0001 whose node key K000 need not be renewed require the renewed node keys $K(t)00$, $K(t)0$, and $K(t)R$. The devices K0000 and K0001 decode the encrypted key $\text{Enc}(K000, K(t)00)$ in the third row from the top shown in Fig. 4(A) to obtain $K(t)00$, decode the encrypted key $\text{Enc}(K(t)00, K(t)0)$ in the second row from the top shown in Fig. 4(A) to obtain the renewed node key $K(t)0$, and decode the encrypted key $\text{Enc}(K(t)0, K(t)R)$ in the first row from the top shown in Fig. 4(A) to obtain $K(t)R$. The devices 0, 1, and 2 can therefore obtain the renewed key $K(t)R$. The index shown in Fig. 4(A) represents the absolute address of the node key and leaf key used as a decoding key.

[0068] In a case where the renewed node keys $K(t)0$ and $K(t)R$ in higher layers of the tree structure shown in Fig. 3 are not required and only the node key K00 need be renewed, an enabling key block (EKB) shown in Fig. 4(B) can be used to distribute the renewed node key $K(t)00$ to the devices 0, 1, and 2.

[0069] The EKB shown in Fig. 4(B) is useful for, for example, distribution of a new content key shared in a particular group. In a specific example, it is assumed that the devices 0, 1, 2, and 3 in a group encircled with a dotted line shown in Fig. 3 use a given recording medium and require a new common content key $K(t)\text{con}$. In this case, data $\text{Enc}(K(t), K(t)\text{con})$ formed by encrypting a new common renewed content key $K(t)\text{con}$ using the renewed $K(t)00$ of the node key K00 common to the devices 0, 1, 2, and 3 is distributed together with the EKB shown in Fig. 4(B). Therefore, this data can be distributed as data which cannot be decoded by a device in other groups, such as the device 4.

[0070] Specifically, the devices 0, 1, and 2 use $K(t)00$ obtained by processing the EKB to decode the above-described encrypted text to obtain a key at the time t , for example, the content key $K(t)\text{con}$ used to encrypt/decode the content.

[3. EKB-based Key Distribution]

[0071] Fig. 5 shows a process for obtaining the key at the time t , for example, the content key $K(t)\text{con}$ used to encrypt/decode the content, showing, for example, the processing of the device 0 which receives the data $\text{Enc}(K(t)00, K(t)\text{con})$ formed by encrypting the new common content key $K(t)\text{con}$ using $K(t)00$, and the EKB shown in Fig. 4(B) by means of a recording medium. In this example, the encrypted message data formed of an EKB is the content key $K(t)\text{con}$.

[0072] As shown in Fig. 5, the device 0 performs the EKB processing, which is similar to that described above, using the EKB at the generation t stored in the recording medium and the node key K000 stored in ad-

vance by the device 0 to generate the node key $K(t)00$. The device 0 further uses the decoded renewed node key $K(t)00$ to decode the renewed content key $K(t)con$, and encrypts the decoded renewed content key $K(t)con$ using the leaf key $K0000$ owned only by the device 0, which is then stored for later use.

[4. EKB Format]

[0073] Fig. 6 shows an example format of an enabling key block (EKB). A version 201 is an identifier indicating the version of the enabling key block (EKB). The version has functions of identifying the latest EKB and indicating the correspondence with the content. A depth indicates the number of layers in the hierarchical tree for the devices to which the enabling key block (EKB) is distributed. A data pointer 203 is a pointer indicating the location of a data section in the enabling key block (EKB), and a tag pointer 204 and a signature pointer 205 are pointers indicating the location of a tag section and a signature, respectively.

[0074] A data section 206 contains data obtained by, for example, encrypting renewed node keys. The data section 206 contains, for example, the encrypted keys of the renewed node keys, etc., shown in Fig. 5.

[0075] A tag section 207 includes tags indicating the positional relationship between the encrypted node keys stored in the data section and the leaf keys. An allocation rule for the tags will be described with reference to Fig. 7. In Fig. 7, the enabling key block (EKB) described above with reference to Fig. 4(A) is sent as data, by way of example. This data is indicated by the table (b) shown in Fig. 7. The address of the top node contained in the encrypted key is referred to as a top node address. In this example, the renewed key $K(t)R$ of the root key is contained, and the top node address is KR . For example, the data $Enc(K(t)0, K(t)R)$ in the top layer is located at position indicated in a hierarchical tree shown in Fig. 7(a). The subsequent data is $Enc(K(t)00, K(t)0)$, and is located at the position left below the previous data in the tree. The tag is set to 0 in case of presence of data, and is set to 1 in case of absence of data. The tags are defined as {left (L) tag, right (R) tag}. The data $Enc(K(t)0, K(t)R)$ in the top row is allocated L tag = 0 because data is located to the left, and is allocated R tag = 1 because data is not located to the right. All the remaining data are allocated tags, and a data string and tag string shown in Fig. 7(c) are configured.

[0076] The tags are allocated in order to indicate at which position of the tree structure data $Enc(Kxxx, Kyyy)$ is located. The key data $Enc(Kxxx, Kyyy) \dots$ stored in the data section is merely a data sequence of encrypted keys. The tags can be used to determine at which position of the tree the encrypted keys stored as data are located. It is possible to configure, for example, the following data structure using the node indexes corresponded with the encrypted data described above with reference to Fig. 4 without tags:

0: $Enc(K(t)0, K(t)root)$
 00: $Enc(K(t)00, K(t)0)$
 000: $Enc(K(t)000, K(T)00)$

5 However, such a data structure using indexes is redundant, i.e., has a large amount of data, and is not suitable for network-based distribution, etc. In contrast, as described above, tags are used as index data indicating the position of keys to determine the position of keys with a smaller amount of data.

10 **[0077]** Referring back to Fig. 6, the EKB format will further be described. A signature 208 includes an electronic signature handled by, for example, a management system having a key management center function, a content server, a license server, a shop server, or the like which issues an enabling key block (EKB). A device which received the EKB checks the signature to determine whether or not the obtained EKB is the enabling key block (EKB) issued by the authorized enabling key block (EKB) issuer.

[5. Category Classification of Tree]

25 **[0078]** A mechanism in which a hierarchical tree structure defining the node keys, etc., is classified into categories of the devices to efficiently renew the keys, distribute the encrypted keys, and distribute the data will be described hereinbelow.

30 **[0079]** Fig. 8 shows an example of category classification in the hierarchical tree structure. In Fig. 8, a root key Kroot 301 is set at the top of the hierarchical tree structure, node keys 302 are set in the lower intermediate layers, and leaf keys 303 are set at the bottom. Each device has an individual leaf key, a series of node keys from the leaf key to the root key, and the root key.

35 **[0080]** As an example, predetermined nodes at the top down to the M-th layer are set as category nodes 304. That is, each of the nodes in the M-th layer is set as a node to which a specific category of device is assigned. One of the nodes in the M-th layer is set as the top, and the nodes in the (M + 1)-th and the following layers and the leaves are the nodes and leaves associated with the devices belonging to this category.

40 **[0081]** For example, a node 305 in the M-th layer shown in Fig. 8 is assigned a category [memory stick (trademark)], and the nodes and leaves which follow this node are set as category-specific nodes or leaves including various devices using a memory stick. Thus, the nodes below the node 305 are defined as a set of nodes and leaves associated with the devices defined in the memory stick category.

45 **[0082]** The nodes in the layers several layers below the M-th layer can be set as sub-category nodes 306. For example, as shown in Fig. 8, a node in the layer two layers below the layer of the category [memory stick] node 305 is assigned a sub-category node belonging to the category of the devices using a memory stick, called a [playback-only device] node. A music playback func-

tion-equipped phone node 307 belonging to the playback-only device category can be configured below the playback-only device node 306 that is a sub-category node, below which a [PHS] node 308 and a [cellular phone] node 309 belonging to the category of music playback function-equipped phones can be configured.

[0083] The categories and sub-categories can be set based on device types as well as arbitrary units, such as unique management nodes of a manufacturer, a content provider, a settlement organization, etc., that is, processing units, management units, or provided service units (these are hereinafter collectively referred to as entities). For example, assuming that a category node is assigned the top node specific to a game device XYZ commercially available from a game device manufacturer, the node keys and leaf keys in the layers below the top node layer can be stored in the game device XYZ commercially available from the manufacturer, and the game device XYZ can be sold. Thereafter, an enabling key block (EKB) formed by the node keys and leaf keys under the top node key is generated and distributed, thus allowing distribution of data such that distribution of encrypted content or distribution or renewal of various keys can be used only on the devices under the top node.

[0084] Accordingly, one node is set as the top, and the node below this node are set as nodes associated with categories or sub-categories assigned to this top node. This enables a manufacturer, a content provider, or the like which manages a top node in a category or sub-category layer to uniquely generate an enabling key block (EKB) having this node as the top and to distribute the generated EKB to the devices belonging to the top node. Therefore, renewal of keys can be carried out without any effect on devices which do not belong to the top node but which belong to another category node.

[0085] In the system of the present invention, as shown in Fig. 9, keys are managed using a system having a tree structure. In the example shown in Fig. 9, nodes in $8 + 24 + 32$ layers form a tree, and the nodes in the eight layers below and including the root node are associated with categories. As used herein, the term category means a category, such as a category such as the category of devices using a semiconductor memory, for example, a memory stick, or the category of digital broadcast receiving devices. One of the category nodes is associated with the present system (referred to as a T-system) serving as a license management system.

[0086] The keys corresponding to the nodes in the 24 layers below the layer of the T-system node are associated with service providers or services provided by the service providers. In this example, therefore, 2^{24} (about 16-mega) service providers or services can be assigned. At the bottom of the 32 layers, 2^{32} (about four-giga) users (or user devices) can be assigned. The key corresponding to the nodes on a path starting with a node in the 32nd layer at the bottom and ending with the T-system node constitute a DNK (Device Node Key),

and an ID corresponding to the leaf at the bottom is referred to as a leaf ID.

[0087] For example, the content key with which the content is encrypted is encrypted using a renewed root key KR', and renewed node keys in a high layer are encrypted using renewed node keys in the layer directly below that layer. These encrypted keys are arranged in an EKB. Renewed node keys in the layer one layer higher than the end in the EKB are encrypted using node keys at the end of the EKB or the leaf keys, and are then arranged in the EKB.

[0088] A user device uses any key of the DNK written in service data to decode the renewed node keys in the layer directly higher than the layer written in the EKB delivered with the content data, and uses the key obtained as a result of decoding to decode renewed node keys in the layer further higher than the layer written in the EKB. The user device performs this operation in turn to obtain the renewed root key KR'.

[0089] As described above, category classification of a tree allows for a mechanism in which one node is set as the top and the nodes which follow the top node are set as nodes associated with a category or sub-category assigned to the top node. This enables a manufacturer, a service provider, etc., which manages a top node in a category or sub-category layer to uniquely generate an enabling key block (EKB) having this node as the top and to distribute the generated EKB to the devices belonging to the top node.

[0090] The mechanism in which the content is distributed and used by using the above-described EKB distribution system by managing devices using a tree structure to realize a multiple-category EKB distribution structure will now be described.

[0091] Two categories will be described below with reference to Fig. 10. As shown in Fig. 10, a T-system node 351 is configured below a root node 350, and a T-service node 352 and a T-hardware node 353 are configured below the T-system node 351. A tree whose top node is the T-hardware node 353 is a category tree in which a user device is set as a leaf 355 and a hardware EKB [EKB(H)] to be issued to the device is delivered. On the other hand, a tree whose top node is the T-service node 352 is a category tree in which a service EKB [EKB(S)] to be issued to a service provided for a user device is delivered.

[0092] Each of the hardware EKB [EKB(H)] and the service EKB [EKB(S)] has a DNK (Device Node Key) assigned to an authorized device, i.e., the keys corresponding to the nodes on a path starting with the leaf and ending with the T-system node, which is used to decode each EKB.

[6. Content Purchase and Preview Process]

[0093] The details of a process for a client to purchase or preview the content will be described with reference to Fig. 11 and the subsequent figures.

[0094] Fig. 11 shows an initial communication sequence of steps in a content purchase process performed between a client having a client application and a browser, such as a PC, and a shop server, a content server, a license server, and a management system. The process shown in the sequence diagram will be described hereinbelow.

[0095] First, a user on the client side who wants to purchase the content specifies a URL (step (1)) on its information processing apparatus having a communication capability, such as a PC, so as to read a content list view (shop page) provided by the shop server via the browser (step (2)) and display the content list view on a display pane (step (3)).

[0096] The client selects the content from the content list provided by the shop server and determines whether the selected content is purchased or previewed (step (4)). Then, the client sends request data to the shop server via the browser (step (5)). The request data contains a content ID (CID), a shop server identifier (Shop ID), and data indicating whether the content is purchased or previewed.

[0097] Upon receipt of the content purchase or preview request from the client, the shop server requests the management system to determine whether or not the content can be provided (step (6)). This request contains a content ID (CID) and a shop server identifier (Shop ID).

[0098] Upon receipt of the request to determine whether or not the content can be provided, the management system issues a transaction ID (TID) (step (7)). The details of the transaction ID (TID) issuing process will be described with reference to the flowchart shown in Fig. 12.

[0099] First, in step S101, the management system generates random numbers, and generates a transaction ID (TID) based on the generated random numbers. In step S102, the generated transaction ID (TID) and the content ID (CID) specified by the shop server are associated with each other, and are stored as transaction data in a storage unit. Then, the generated transaction ID (TID) is output and issued to the shop server.

[0100] Referring back to the sequence diagram shown in Fig. 11, after generating the transaction ID (TID), the management system sends the generated transaction ID (TID) and price information, as TID information, to the shop server (step (8)). The price information is information requested only for purchasing the content, and is not contained in the content preview process. The shop server which has received the TID information performs a billing process (step (9)) based on the price contained in the TID information when a content purchase request was made by the client.

[0101] When a content preview request, not a content purchase request, was made by the client, the billing process (step (9)) is omitted.

[0102] The subsequent process will be described with reference to the sequence diagram shown in Fig. 13.

The shop server sends a download permission request for the content to be purchased or previewed to the management system on the condition that, in the content purchase process, the billing process has been performed or on the condition that, in the content preview process, the TID information has been received from the management system (step (10)).

[0103] Upon receipt of the download permission request, the management system verifies the download permission request (step (11)). The details of the download permission request verification process will be described below with reference to the flowchart shown in Fig. 14.

[0104] First, in step S201, the management system matches the transaction ID (TID) contained in the received download permission request with the transaction ID (TID) previously generated and stored in the storage unit. In step S202, the management system obtains the content ID (CID) recorded in association with the verified transaction ID (TID), and, in step S203, issues a download permission of the content corresponding to the CID.

[0105] Referring back to the sequence diagram shown in Fig. 13, after checking the download permission request (step (11)), the management system issues a content download permission to the shop server (step (12)). The download permission contains a transaction ID (TID), a content server URL (C-URL), a license server URL (L-URL), a content ID (CID), a usage-right information ID (UID), an item (content) URL (S-URL), and a service ID.

[0106] Upon receipt of the download permission from the management system, the shop server generates a start-up file for starting a content using (playback, etc.) program in the client application, and sends the generated start-up file to the client application via the browser of the client.

[0107] An example of the start-up file will be described with reference to Fig. 15. A start-up file 360 contains the transaction ID (TID) generated by the management system, the content ID (CID) of the content to be purchased or previewed by the client, the usage-right information ID (UID) contained in the download permission information generated by the management system, the service ID contained in the download permission information generated by the management system, the URL of the license server, the URL of the item (content), and identification data indicating a content purchase or preview process.

[0108] The identification data indicating a content purchase or preview process may be configured such that identifiers for the purchase process and the preview process differ from each other and the client application determines which identifier is set in the start-up file to start an appropriate one of the purchase and preview applications.

[0109] The client application starts the application depending upon the start-up file (step (15)).

[0110] The application starting process performed by the client application will be described with reference to Fig. 16. First, in step S301, it is determined whether or not the client system, or the information processing apparatus, has the service data corresponding to the service ID contained in the start-up file.

[0111] The service data is received from the license server when the client wants to receive various services, for example, a content-using service, and is, for example, data which authorizes the overall service usage right of the services provided by a specific service provider. An example data structure of the service data is shown in Fig. 17(a).

[0112] As shown in Fig. 17(a), service data 370 contains a leaf ID unique to a client set in an EKB distribution tree, a service ID serving as a service identifier, and data E(Kroot, DNK) formed by encrypting a device node key (DNK) using a root key (Kroot). In order to receive the service data, the client must be registered in the license server. The registration process is indicated in steps (15) and (16) shown in Fig. 13.

[0113] If it is determined in step S301 shown in Fig. 16 that the client does not have the service data corresponding to the service ID, a registration process is performed in step S302 to receive the service data.

[0114] In the registration process, default usage-right information is issued to the client from the license server. Standard usage-right information contains usage rules and conditions of the purchased content, and is issued when the content is purchased; whereas, the default usage-right information is not issued on the condition that the content is purchased, but is issued on the condition that the client is registered or the service data is issued. The default usage-right information is used as content usage-right information for effective use in the content preview process, as described below.

[0115] An example data structure of the usage-right information is shown in Fig. 17(b). As shown in Fig. 17(b), usage-right information 371 contains a usage-right information ID serving as a usage-right information identifier, a timestamp serving as information indicating the time and date of issuance, a leaf ID unique to the client, a content ID, if the information is issued for content purchase, and usage-rule-defined content type information.

[0116] Since the default usage-right information is not issued for specific purchased content, the content ID is omitted, or is replaced by an ID commonly used for the content which can be previewed. The usage-rule-defined content type information is configured such that, for example, the content whose preview flag is set to ON can be used. As shown in Fig. 17(c), content 372 includes a preview flag 373. The content whose preview flag 373 is set to ON indicates the content which can be previewed, and the content whose preview flag is set to OFF indicates the content which cannot be previewed.

[0117] For playback of preview-content, the client application refers to the default usage-right information to

determine whether or not the content can be played back, and verifies the flag of the content to play back the content. This process is described below.

[0118] Referring back to the flowchart shown in Fig. 16, the procedure for starting an application will be described. After the registration process in step S302, that is, after the service data and the default usage-right information has been obtained from the license server, it is determined in step S303 whether the start-up file received from the shop server is a start-up file for a purchase application or a start-up file for a preview application. If it is a start-up file for a purchase application, the purchase application is executed in step S304. If it is a start-up file for a preview application, the preview application is executed in step S305.

[0119] A sequence of steps for executing the purchase application will be described with reference to the sequence diagram shown in Fig. 18.

[0120] In the purchase process, the client application sends a content download request to the content server (step (21)). A purchase request of this content has been sent from the client, and the content corresponds to the content ID (CID) recorded in the usage-right information (see Fig. 17(b)). The client application specifies content based on the content ID (CID) to send a download request of the content to the content server.

[0121] Upon receipt of the content download request, the content server sends content information corresponding to the CID to the client (step (22)). The content information contains the encrypted content, and is formed of a file in which the content data Enc(Kc, Content) encrypted using a content key Kc, the data Enc(Kroot, Kc) formed by encrypting the content key Kc using a root key Kroot, the EKB for obtaining the root key Kroot, and information, such as the preview flag data and the service ID, shown in Fig. 17(c), are added.

[0122] The client which has received the content information sends a request for obtaining usage-right information (Usage Right) corresponding to the received content to the license server (step (23)). The request contains the usage-right information ID (UID) contained in the start-up file (see Fig. 15) previously received from the shop server, the leaf ID serving as client identification data, and the transaction ID (TID) contained in the start-up file (see Fig. 15) previously received from the shop server.

[0123] Upon receipt of the usage-right information (Usage Right) obtaining request, the license server sends an order inquiry to the management system (step (24)). This request contains the usage-right information ID (UID) and the transaction ID (TID). Upon receipt of the order inquiry, the management server sends response information defining the usage rules corresponding to the usage-right information ID (UID) to the license server in response to the order inquiry (step (25)).

[0124] Upon receipt of the response information, the license server generates usage-right information (Us-

age Right) having content usage rules, and issues the generated usage-right information to the client (step (26)). The content usage rules are formed of the time the content can be played back, the expiry, and permission information of various operations, such as content copying and checkout to an external device.

[0125] The client which has received the usage-right information (Usage Right) is able to use the content previously received from the content server based on the usage rules recorded in the usage-right information (Usage Right). When a content playback request is sent from the user while specifying a content ID (CID) and a usage-right information (Usage Right) ID (step (27)), the client application performs a content playback process according to the usage rules (step (28)).

[0126] A basic content playback procedure will be described with reference to Fig. 19. As is anticipated from the foregoing description, content is provided for a client 383 by a content server 382, and service data and usage-right information (Usage Right) are licensed from a license server 381 to the client 383.

[0127] The content has been encrypted using a content key Kc, i.e., $\text{Enc}(\text{Kc}, \text{Content})$, and the content key Kc is a key obtained from a root key Kroot which can be obtained from an EKB.

[0128] The client 383 obtains a device node key (DNK) from the service data received from the license server, and decodes an EKB in a content file based on the obtained DNK to obtain the root key Kroot. The client 383 further uses the obtained root key Kroot to decode $\text{Enc}(\text{Kroot}, \text{Kc})$ to obtain the content key Kc, and decodes the encrypted content $\text{Enc}(\text{Kc}, \text{Content})$ using the obtained content key Kc to obtain the content for playback.

[0129] The details of a content playback process in association with service data and usage-right information (Usage Right) will be described with reference to Fig. 20.

[0130] Fig. 20 is a sequence diagram showing a content-using process based on a content decoding process using a hardware EKB [EKB(H)] and a service EKB [EKB(S)].

[0131] Service data 401 and usage-right information 403 shown in Fig. 20 are data received from a license server, and an encrypted content file 402 is data received from a content server. The service data 401 contains a leaf ID serving as a leaf identifier, the version of the used EKB, and data $\text{E}(\text{Kroot}', \text{SDNK})$ formed by encrypting a service-specific device node key (SDNK) necessary to decode a service EKB [EKB(S)] using a root key Kroot' assigned in a hardware category tree.

[0132] The encrypted content file 402 is a file containing a service EKB [EKB(S)] having a root key Kroot assigned in a service category tree, data $\text{E}(\text{Kroot}, \text{CID} + \text{Kc})$ formed by encrypting a content ID (CID) and a content key (Kc) used for the content encrypting and decoding processes using the root key Kroot, and data $\text{E}(\text{Kc}, \text{Content})$ formed by encrypting the content (Content) using

the content key Kc.

[0133] The usage-right information 403 is data containing a leaf ID and usage-rule information of the content. The usage-rule information of the content includes various usage rules, such as a use period which is defined depending upon the content, the time the content can be used, and copy control. A user device which has received the usage-right information 403 stores the usage-right information as security information of the content, or stores the usage-right information in an AV index file serving as content index data.

[0134] A user device having a large-capacity storage unit and a high-performance processor, such as a PC, can store usage-right information as security information of the content. Preferably, such a user device stores all usage-right information, and refers to the usage-right information stored therein to use the content. On the other hand, a user device which does not have a large-capacity storage unit and which has a low-performance processor, such as a portable device (PD), can store the usage-right information 403 formed of selected information in an AV index file serving as content index data, and can refer to the usage-rule information in the AV index file to use the content.

[0135] In step S501 shown in Fig. 20, the user device uses a hardware device node key (HDNK) 412 to decode a hardware EKB(H) 411 to obtain a root key Kroot' assigned in a hardware category tree from the EKB(H) 411. The DNK-based EKB process corresponds to a process in accordance with the technique described above with reference to Fig. 5.

[0136] In step S502, the root key Kroot' obtained from the EKB(H) is used to decode the encrypted data $\text{E}(\text{Kroot}', \text{SDNK})$ of the service data 401 to obtain a device node key (SDNK) used for processing (decoding) the service EKB [EKB(S)].

[0137] In step S503, the device node key (SDNK) obtained from the service data is used to process (decode) the service EKB [EKB(S)] stored in the encrypted content file 402 to obtain a root key Kroot assigned in the service category tree stored in the service EKB [EKB(S)].

[0138] In step S504, the root key Kroot obtained from the service EKB [EKB(S)] is used to decode the encrypted data $\text{E}(\text{Kroot}, \text{CID} + \text{Kc})$ stored in the encrypted content file 402 to obtain a content ID (CID) and a content key (Kc).

[0139] In step S505, the content ID (CID) obtained from the encrypted content file 402 is matched with the content ID stored in the usage-right information. When it is determined as a result of matching that the content can be used, in step S506, the content key (Kc) obtained from the encrypted content file 402 is used to decode the encrypted content $\text{E}(\text{Kc}, \text{Content})$ stored in the encrypted content file 402 to play back the content.

[0140] As described above, the hardware EKB [EKB(H)] serving as an EKB corresponding to a category tree established for hardware devices, which are content-us-

ing devices, and the service EKB [EKB(S)] serving as an EKB corresponding to a category tree established for content-using services, can be individually provided for a user, thus allowing only the user having the authorized DNK for each EKB to use the services.

[0141] A DNK for decoding a service EKB [EKB(S)], i.e., an SDNK, can be provided as the service data 401 corresponding to the content, and the SDNK is encrypted using a root key Kroot' assigned in a hardware category tree which can be obtained only by a device having an authorized hardware DNK, i.e., an HDNK. This allows only a user device having the authorized HDNK to obtain the SDNK and to use the services.

[0142] In using the content, the content identifier (CID) obtained from the encrypted content file 402 is matched with the CID obtained from the usage-right information. It is therefore essential to the content playback process to obtain the usage-right information 403 having the CID information. This can realize content use in accordance with the usage rules.

[0143] The process in a case where the client application executes a preview application will be described with reference to the sequence diagram shown in Fig. 21.

[0144] In the preview process, like the content purchase process, it is possible to obtain the content information file (see Fig. 19) and store it in a storage unit of the client system before the content is played back in a similar manner to purchased content; however, an example where a streaming playback is performed without storage in the storage unit will be described with reference to Fig. 21.

[0145] In the streaming preview process, the client application sends a content download request to the content server (step (31)). A preview request of this content has been sent from the client. The client application specifies content based on the content ID (CID) to send a download request of the content to the content server.

[0146] In streaming playback, the content server sequentially sends partial data of the content (content part) to the client (step (32)). The client which has received the content part plays back the received content part (step (33)), and sends a request of the remaining content parts to the content server. This process is consecutively performed to achieve streaming playback.

[0147] A preview playback procedure will be described with reference to the flowchart shown in Fig. 22. In step S701, the client application obtains a service ID from a preview content file received from the content server.

[0148] In step S702, it is determined whether or not default usage-right information (Default Usage Right) (see Fig. 17(b)) corresponding to the extracted service ID is present. The default usage-right information is usage-right information which is sent together with the service data (see Fig. 17(a)) from the license server when the client is registered and which is used for the content which can be previewed, unlike the usage-right

information issued for purchased content.

[0149] The content can be previewed on the condition that the default usage-right information (Default Usage Right) is possessed. If the default usage-right information is not possessed, an error occurs in step S705, and the process ends without playing back the content.

[0150] If the default usage-right information (Default Usage Right) has been stored, in step S703, the default usage-right information is verified to check the recorded usage right. The default usage-right information contains, for example, preview permission information of the content whose preview flag is on, and content ID information of the content which can be previewed, and such information is retrieved.

[0151] In step S704, the content is played back based on the usage rules of the default usage-right information (Default Usage Right). As described above with reference to Figs. 19 and 20, the playback process involves a process for decoding the encrypted content received from the content server.

[0152] Like the process for playing back the purchased content described with reference to Fig. 20, also in previewing the content without purchasing the content, the EKB-based key obtaining process is required for obtaining the keys for decoding the content. This allows, for example, only the user having the authorized DNKs for the hardware EKB [EKB(H)] serving as an EKB corresponding to a category tree established for hardware devices, which are content-using devices, and the service EKB [EKB(S)] serving as an EKB corresponding to a category tree established for content-using services to play back the content, and to also preview the content with limited playback control.

[0153] As described above, the client obtains the default usage-right information (Default Usage Right) when it is registered to the license server, and can play back the content based on the default usage-right information in the content preview process without purchasing the content, thus allowing the user to preview and play back the content without purchasing the content. The client which is permitted to preview the content is limited to a client which has been registered to the license server to obtain the default usage-right information. This prevents preview-data from being randomly distributed.

[0154] Streaming playback is shown in the sequence diagram shown in Fig. 21, by way of example. However, preview-data may be stored in a storage medium of the client and may be played back by determining whether or not default usage-right information (Default Usage Right) is present and based on the data recorded in the default usage-right information.

[7. Backup/Restoration Process]

[0155] A backup and restoration processes of the content purchased by the client or content usage-right information will now be described.

[0156] The restoration process is performed in order to re-obtain the license information corresponding to the content, that is, the service data, to re-obtain and store the usage-right information, or to re-obtain the content when or after the client purchases the content.

[0157] In one form of the restoration process, any or all of the service data, the usage-right information, and the content can be re-obtained. In the following example, a sequence of process steps for re-obtaining and storing all of the service data, the usage-right information, and the content is described, by way of example; however, all data is not necessarily re-obtained, and any of the data may be selectively re-obtained.

[0158] The details of the backup/restoration process will be described with reference to Fig. 23 and the subsequent figures. Fig. 23 shows an initial communication sequence of steps in the backup/restoration process performed between a client having a client application and a browser, such as a PC, and a shop server, a content server, a license server, and a management system. The process shown in the sequence diagram is described hereinbelow.

[0159] It is assumed that the client purchased content in an authorized manner according to the above-described content purchase process. The sequence shown in Fig. 23 is a sequence of steps subsequent to the content purchase process.

[0160] The client which purchased the content generates a data file for obtaining backup/restoration data, that is, a restoration request file [restore.dat] (step (50)). The structure of the restoration request file [restore.dat] is shown in Fig. 24.

[0161] As shown in Fig. 24, the restoration request file [restore.dat] is formed of a leaf ID serving as client identification data in an EKB distribution tree, and a hash value, for example, verification data having a MAC (Message Authentication Code). The client application uses a secret key shared with the management system to calculate the hash value or the MAC, which is verification data based on the leaf ID, to generate the restoration request file [restore.dat] formed of the leaf ID and the verification data.

[0162] The message authentication code (MAC) is generated as data for determining whether or not the data is tampered with. An example of a process for generating a MAC value by means of DES encryption is shown in Fig. 25. As shown in Fig. 25, a message to be processed is divided into parts each consisting of eight bytes (the divided parts of the message are hereinafter denoted by M1, M2, ..., MN). First, the exclusive-OR between an initial value (hereinafter referred to as IV) and M1 is calculated (wherein the result is indicated by I1). Then, I1 is input to a DES encoder to encrypt it using a key (hereinafter denoted by K1) (wherein the resultant output is indicated by E1). Then, the exclusive-OR between E1 and M2 is calculated, and the resultant output I2 is input to the DES encoder to encrypt it using the key K1 (the resultant output is indicated by E2). The above-

described operation is repeated until all parts of the message are encrypted. The final output EN is employed as a message authentication code (MAC).

[0163] The MAC value has a different value if source data for generating the MAC changes. A MAC generated based on the data (message) to be verified is matched with the recorded MAC. If both MACs match, it is proved that the data (message) to be verified is not modified or tampered with.

[0164] Referring back to the sequence diagram shown in Fig. 23, the client accesses a restoration page provided by the management system via the browser (step (51)), and the management system provides the restoration page for the browser of the client (step (52)).

The restoration page provided by the management system is a page having an uploading function of the restoration request file [restore.dat].

[0165] On the restoration page provided by the management system, the client uploads the restoration request file [restore.dat] generated by the client application. As described above with reference to Fig. 24, the restoration request file [restore.dat] is formed of a leaf ID serving as a client identification data in an EKB distribution tree, and a hash value having, for example, a MAC (Message Authentication Code).

[0166] Upon receipt of the restoration request file [restore.dat], the management system uses a secret key shared with the client to determine a hash value for the leaf ID, and matches the determined hash value with the received hash value to verify the received data (step (54)). On the condition that the determined hash value matches the received hash value, a start-up file for backup/restoration is sent to the client (step (55)). The start-up file has the file structure similar to that described above with reference to Fig. 15.

[0167] The start-up file is passed from the browser to the client application (step (56)) to start a backup/restoration execution program, which is determined and selected depending upon a script or an extension of the start-up file to perform a restoration process (step (57)).

[0168] The objects to be backed up/restored are service data, content, and content usage-right information. As described above, the service data can be obtained by registering the client to the license server, and the content can be obtained from the content server. The usage-right information is obtained from the license server. In the backup/restoration process, such data are also obtained from the respective servers.

[0169] A process for obtaining service data for backup/restoration is first described with reference to Fig. 26. This process is basically performed in accordance with a procedure similar to that in the above-described client registration process for content purchase.

[0170] First, the client application sends a registration request to the license server (step (61)). The registration request includes the transaction ID (TID) contained in the start-up file generated by the management system.

[0171] The license server which has received the reg-

istration request identifies the process for obtaining service data for backup/restoration based on the transaction ID (TID), and sends an allocation request of pre-service data, that is, backup/restoration data of the service data, to the management system (step (62)). The management system determines, based on management data, whether or not there is any client terminal which executed processing based on the same transaction ID. If such a client terminal exists, the management data in association with the client terminals is stored (step (63)). This can prevent processing when a limited time (for example, three times) the backup/restoration process is carried out and if a request is made in excess of the upper limit.

[0172] The management system which has updated the management data sends a response to the pre-service data allocation request to the license server (step (64)). This response is sent as permission information to issue backup/restoration service data.

[0173] The license server which has received the pre-service data allocation response issues backup/restoration service data to the client (step (65)). As described above with reference to Fig. 17(a), the service data 370 includes a client-unique leaf ID assigned in the EKB distribution tree, a service ID serving as a service identifier, and data $E(\text{Kroot}, \text{DNK})$ formed by encrypting a device node key (DNK) using a root key (Kroot).

[0174] During this operation, the default usage-right information (see Fig. 17(b)) is also issued to the client from the license server. As described above, standard usage-right information contains usage rules and conditions of the purchased content, and is issued when the content is purchased; whereas, the default usage-right information is not issued on the condition that the content is purchased, but is issued on the condition that the client is registered or the service data is issued. As described above, the default usage-right information is used as usage-right information for effective use in the content preview process.

[0175] The client which has received the service data and default usage-right information from the license server stores such data in a storage unit for backup (step (66)).

[0176] The content backup/restoration process will be described with reference to Fig. 27. In the content backup/restoration process, the client application sends a content download request to the content server (step (71)). The content is the same as the content previously purchased by the client. The client application specifies content based on the content ID (CID) to send a download request of the content to the content server.

[0177] Upon receipt of the content download request, the content server sends content information corresponding to the CID to the client (step (72)). The content information is information containing the encrypted content. As described above with reference to Fig. 17(c), the content information is a file in which the content data $\text{Enc}(\text{Kc}, \text{Content})$ encrypted using a content key Kc, the

data $\text{Enc}(\text{Kroot}, \text{Kc})$ formed by encrypting the content key Kc using a root key Kroot, the EKB for obtaining the root key Kroot, and information, such as the preview flag data and the service ID, are added.

5 [0178] The client which has received the content information sends a request for obtaining usage-right information (Usage Right) corresponding to the received content to the license server (step (73)). The request contains the usage-right information ID (UID) contained in the start-up file (see Fig. 15), the leaf ID serving as client identification data, and the transaction ID (TID).

10 [0179] Upon receipt of the usage-right information (Usage Right) obtaining request, the license server sends an order inquiry to the management system (step (74)). This request contains the usage-right information ID (UID) and the transaction ID (TID). Upon receipt of the order inquiry, the management server sends response information having the usage rules corresponding to the usage-right information ID (UID) to the license server in response to the order inquiry (step (75)).

15 [0180] Upon receipt of the response information, the license server generates usage-right information (Usage Right) having content usage rules, and re-issues the generated usage-right information to the client (step (76)). The content usage rules are formed of the time the content can be played back, the expiry, and permission information of various operations, such as content copying and checkout to an external device.

20 [0181] The client which has received the usage-right information (Usage Right) stores the previously received content and usage-right information in a storage unit as backup data.

25 [0182] The usage-right information issued by the license server in the backup/restoration process may contain different usage rules from those of the usage-right information issued when authorized content is purchased. Such usage rules may include, for example, more limited conditions than the usage rules contained in the usage-right information issued when authorized content is purchased, such as a limited use period, copy-prohibited, or checkout-prohibited, and the usage-right information for backup/restoration containing such usage rules may be issued.

45 [8. Secondary Distribution of Content Based on Recommendation File]

50 [0183] A mechanism in which the client which purchased content in an authorized manner provides the purchased content for another client, i.e., so-called secondary distribution of the content is performed, and a content usage right is newly delivered from the license server so that the client which has received the secondarily distributed content can also use the content on the condition that the client has the authorized content usage right, while reducing the load on the content server which distributes the content, will now be described.

55 [0184] As described above, the client which plays

back the content for use must receive encrypted content from the content server and must also receive license information, that is, service data and usage-right information corresponding to the content, from the license server in order to use the content.

[0185] Since the license information, i.e., the service data and the usage-right information, has a small amount of data, a large amount of traffic is not generated even if such information is exchanged frequently over a communication network such as the Internet, and does not cause a problem in that it takes a long time to transfer the information. However, the content including various kinds of data, such as music data, image data, and programs, has a large amount of data. When such a large content is transmitted from a specific content server to multiple clients, various problems occur in that the transmission time is long, the load on the content server increases, a large amount of network traffic is generated, etc. There can occur another problem that a communication error causes a content distribution error during communication.

[0186] A system in which a client which purchased the authorized content provides the content for another client, i.e., secondarily distributes the content, and the client which has received the secondarily distributed content receives license information of the content from the license server, thus reducing the load on the content server which sends the content to the client is described hereinbelow.

[0187] Fig. 28 is a flowchart showing a procedure for generating a content file provided by a client which received content in an authorized manner for another client. A data file including the content provided for another client is referred to as a recommendation file. The recommendation file contains a content file including the encrypted content, and, if necessary, a description file (for example, an HTML file) of the content.

[0188] The process shown in the flowchart of Fig. 28 is described hereinbelow. A client which performs the process shown in Fig. 28 is a client which performed the above-described content purchase process to purchase the content in an authorized manner, or a client which received the recommendation file from another client to obtain the authorized license in the subsequent procedure. The process shown in Fig. 28 is carried out by executing one execution program of the client application (the client application 12 shown in Fig. 1) under control of a controller (a CPU, etc.) of an information processing apparatus serving as a client system. In step S801, the client displays a recommendation-file creation view on a display of its client device.

[0189] An example recommendation-file creation view is shown in Fig. 29. A content list 651 of pieces of content which were purchased in an authorized manner by the client and which can be played back is displayed in the center window. When a recommendation file is generated, a piece of content is selected from the content list 651 (step S802), and the title, etc., of the select-

ed piece of content is shown in a list 654 displayed in the right window. Movement of the piece of content between the content list 651 and the list 654 is executed by operating drag switches 652 and 653.

5 [0190] When the piece of content whose recommendation file is to be generated is selected, in step S803, a recommendation-file creation button 655 is clicked. When the recommendation-file creation button 655 is clicked, it is determined in step S804 whether or not a description file, for example, an HTML description file, is generated and stored in the recommendation file together with the content file. This is selectable by the user.

10 [0191] There are two types of recommendation files; a recommendation file 720 shown in Fig. 30(a) has a combination of a content file 721 including the encrypted content and a content description file 722, and a recommendation file 730 shown in Fig. 30(b) has a content file 721 including the encrypted content alone. The client is free to select either type.

15 [0192] If it is determined in step S804 that a content description file is not created, the recommendation file 730 having the content file 721 alone, shown in Fig. 30(b), is generated.

20 [0193] The structure of the content file is shown in Fig. 31. The content file (MQT file) 721 includes the encrypted content, meta-information serving as additional content information, a shop-server URL indicating the shop from which the content can be purchased, and a content ID (CID) serving as a content identifier.

25 [0194] The encrypted content contained in the content file is the content encrypted using a content key Kc, and the content key Kc is a key which can be obtained only by using a key which can be obtained by decoding an enabling key block (EKB) provided using an enabling key block (EKB) distribution tree structure.

30 [0195] If it is determined in step S804 that a content description file is created, in step S806, description data (meta-data) for generating the content description file (HTML file) is retrieved from a content management table. Although, as described above, the content description data corresponding to the content is also contained in the content file together with the encrypted content, the client which obtained the content usage right in an authorized manner has stored and managed the content meta-data retrieved from the content file as content management data in a separate file. The meta-data for the description file generated in the recommendation file is extracted from the content management data.

35 [0196] In step S807, the meta-data extracted from the content management data is added to a template HTML file set in the client application to generate an HTML file for content description. In step S808, a recommendation file having a combination of the content file and the HTML file for description is generated.

40 [0197] An example view of the HTML file serving as a content description data is shown in Fig. 32. In the example shown in Fig. 32, the content is music data. As shown in Fig. 32, the description file includes a music

content list of song titles, artists, and agents, and description of various operations and processes. The client which has received the recommendation file from another client first opens the description file.

[0198] The content contained in the recommendation file is encrypted content, and cannot be played back unless the authorized license information, i.e., the service data and the usage-right information corresponding to the content, is obtained. Therefore, the client which has received the recommendation file must execute a license information obtaining procedure in order to use the content stored in the recommendation file.

[0199] The license information obtaining process will be described with reference to the process flowcharts shown in Figs. 33 and 34. The client which has received the recommendation file opens the description file (HTML file) shown in Fig. 32, and clicks a preview/purchase content delivery site button 731 (step S811). This clicking operation allows the client application to start (step S812) so as to retrieve the content file (MQT file) (see Fig. 31) stored in the same recommendation file to extract the content ID (CID) and the shop URL from the content file (step S813).

[0200] The preview/purchase content delivery site button 731 of the content description file is therefore formed as link data for starting a client application program for extracting the shop-server URL from the content file and outputting the extracted URL to the browser. This enables the client which has received the recommendation file to easily access the shop to perform the purchase process.

[0201] In step S814, a content file name is configured based on the content ID (CID) extracted from the content file. This file name configuration process is set in advance in the client application, in which, for example, the title of the content, the name of artist, combination data thereof, or the like is employed. In step S815, the content file having the file name configured in step S814 is stored in the storage unit of the client.

[0202] In step S816, the shop URL extracted from the content file in step S813 is transferred to the browser, and the browser reads the shop page corresponding to the received URL from the shop server.

[0203] In step S831 in the process shown in the flowchart of Fig. 34, a shop view is shown in the client display. The subsequent operations are basically similar to any of the above-described content purchase and preview processes, and are performed according to the procedure described above with reference to Figs. 11, 13, 18, and 21. However, the content itself has been already retrieved by the client from the recommendation file, and the process for receiving the content from the content server is thus omitted.

[0204] The overview of a series of operations is shown in step S832 and the following steps of the process flowchart shown in Fig. 34. First, when the client specifies purchase in the shop view provided by the shop server and outputs a purchase request to the shop

server, a purchase start-up file is sent from the shop server. The purchase start-up file has a structure similar to that of the start-up file described above with reference to Fig. 15.

[0205] In step S833, the content ID (CID) serving as a content identifier is retrieved from the start-up file. In step S834, a content file name is determined based on the content ID (CID). As described above with reference to the flowchart shown in Fig. 33, it is defined in the client application that the content file name necessary for storing the content in the client device is configured based on the content ID (CID), and the CID and the file name are associated with each other.

[0206] In step S835, it is determined whether or not the file having the same file name as the file name determined from the content ID (CID) has been stored in the storage unit of the client device. If the content has not been stored, in step S837, the client device accesses the content server to download the content. This operation is similar to that in the above-described content purchase process.

[0207] Meanwhile, the client which received the recommendation file has stored in the storage unit the content file having the predetermined file name configured in steps S814 and S815 in the flowchart shown in Fig. 33, and the content usage-right information process is performed in step S836, without the content downloading process. Then, the process ends.

[0208] When the client plays back the content, as described above, the content identifier (CID) stored in the content usage-right information is matched with the content identifier (CID) of the content to be played back, and the content is played back on the condition that the CIDs match. The content can be played back and used by decoding an enabling key block (EKB) provided using an enabling key block (EKB) distribution tree structure to obtain a content key Kc, and by using the obtained content key Kc to decode the encrypted content.

[0209] Accordingly, the client having the content provides the recommendation file formed of the content file including the encrypted content and the description file for another client, thus allowing the other client to receive the content without access to the content delivery server. The other client is able to use the content on the condition that the usage-right information has been obtained. This prevents unauthorized use of the content.

[0210] Although the service data obtaining process is omitted in the flowchart shown in Fig. 34, when a client having no service data receives a recommendation file, the client must access the license server to perform a registration process to obtain the service data. The registration process corresponds to the process described above with reference to Figs. 13 and 16.

[0211] The present invention has been described in detail with reference to a specific embodiment. However, it is obvious that modifications or replacements may be made to this embodiment by those skilled in the art without departing from the spirit and scope of the

present invention. The present invention has been disclosed in an exemplary form, and this form should be construed as the restricted one. Reference should be made to the CLAIM for delineation of the scope of the present invention.

[0212] The series of operations described herein can be executed by hardware or software, or a combination thereof. In a case where the operations are executed by software, a program containing a sequence of the operations may be installed in an internal memory of a computer incorporated in dedicated hardware to execute the program, or the program may be installed in a general-purpose computer capable of performing various operations to execute the program.

[0213] For example, the program can be recorded in advance in a storage medium such as a hard disk or a ROM (Read Only Memory). Alternatively, the program can be temporarily or persistently stored (recorded) in a removable recording medium, such as a flexible disk, a CD-ROM (Compact Disc Read Only Memory), an MO (Magnetooptical) disk, a DVD (Digital Versatile Disc), a magnetic disk, or a semiconductor memory. Such a removable recording medium can be offered as so-called packaged software.

[0214] The program may be installed in a computer from the above-noted removable recording media, or may also be wirelessly transferred to a computer from a download site or transferred to a computer via a line over a network such as a LAN (Local Area Network) or the Internet. The computer can receive the thus transferred program, and can install the program in an internal storage medium such as a hard disk.

[0215] The various operations described herein may be performed in a time-series manner according to the description, or may also be performed in parallel or independently depending upon the performance of the device that performs the operations or depending upon necessity.

Industrial Applicability

[0216] According to the structure of the present invention, therefore, a client obtains default usage-right information (Default Usage Right) when it is registered to a license server, and is permitted to play back the content based on the default usage-right information in a content preview process without purchasing the content. Therefore, the user is able to preview and play back the content without purchasing the content. The client which is permitted to preview the content is limited to a client which has been registered to the license server to obtain the default usage-right information. This prevents preview-data from being randomly distributed.

[0217] According to the structure of the present invention, furthermore, also in the content preview process without purchasing the content, only the user having authorized DNKs for a hardware EKB [EKB(H)] serving as an EKB corresponding to a category tree established for

hardware devices, which are content-using devices, and a service EKB [EKB(S)] serving as an EKB corresponding to a category tree established for content-using services can play back the content and preview the content with limited playback control.

Claims

1. An information processing apparatus for controlling decoding and using of encrypted content, said information processing apparatus comprising:

control means for controlling content use based on usage-right information (usage right) corresponding to the content according to an instruction to use the content; and
recording means for recording default usage-right information, the default usage-right information being recorded in manufacturing or being obtained at a service registration time,

wherein said control means permits the content to be decoded and used based on the description of the default usage-right information when the content includes information indicating association with the default usage-right information.

2. An information processing apparatus according to Claim 1, wherein the content which is permitted for use based on the default usage-right information is provided for the purpose of sampling, and

said control means determines whether or not the content includes a flag indicating sample content, and permits playback of the content according to a determination result.

3. An information processing apparatus according to Claim 1, further comprising:

sending means for sending a service registration request; and
receiving means for receiving the default usage-right information sent from a license server in response to the registration request.

4. An information processing apparatus according to Claim 3, wherein said receiving means further receives key information necessary for decoding the content.

5. An information processing apparatus for issuing a usage right having usage rules of encrypted content, said information processing apparatus comprising:

receiving means for receiving a registration re-

quest; and
 sending means for sending key information and
 default usage-right information in response to
 the registration request, the key information be-
 ing necessary for decoding the encrypted con-
 tent.

6. An information processing apparatus according to
 Claim 5, wherein the content which is permitted for
 use based on the default usage-right information is
 provided for the purpose of sampling, and

the default usage-right information includes a
 description indicating that playback of the con-
 tent is permitted when the content includes a
 flag indicating sample content.

7. An information processing method for controlling
 decoding and using of encrypted content, said in-
 formation processing method comprising a control
 step of controlling content use based on usage-right
 information (usage right) corresponding to the con-
 tent according to an instruction to use the content,
 wherein said control step includes:

a step of determining whether or not the content
 includes information indicating association with
 default usage-right information recorded in
 manufacturing or default usage-right informa-
 tion obtained at a service registration time; and
 a step of permitting the content to be decoded
 and used based on the description of the de-
 fault usage-right information when the content
 includes the information indicating association
 with the default usage-right information.

8. An information processing method according to
 Claim 7,
 wherein the content which is permitted for use
 based on the default usage-right information is pro-
 vided for the purpose of sampling, and

said control step further includes a step of de-
 termining whether or not the content includes a
 flag indicating sample content, and permitting
 playback of the content according to a determi-
 nation result.

9. An information processing method according to
 Claim 7, further comprising:

a sending step of sending a service registration
 request; and
 a receiving step of receiving the default usage-
 right information sent from a license server in
 response to the registration request.

10. An information processing method according to

Claim 9, further comprising a step of receiving key
 information necessary for decoding the content.

11. An information processing method for issuing a us-
 age right having usage rules of encrypted content,
 said information processing method comprising:

a receiving step of receiving a registration re-
 quest; and

a sending step of sending key information and
 default usage-right information in response to
 the registration request, the key information be-
 ing necessary for decoding the encrypted con-
 tent.

12. An information processing method according to
 Claim 11, wherein the content which is permitted for
 use based on the default usage-right information is
 provided for the purpose of sampling, and

the default usage-right information includes a
 description indicating that playback of the con-
 tent is permitted when the content includes a
 flag indicating sample content.

13. A computer program for performing an information
 process for controlling decoding and using of en-
 crypted content, said computer program including
 a control step of controlling content use based on
 usage-right information (usage right) correspond-
 ing to the content according to an instruction to use
 the content,

wherein said control step includes:

a step of determining whether or not the content
 includes information indicating association with
 default usage-right information recorded in
 manufacturing or default usage-right informa-
 tion obtained at a service registration time; and
 a step of permitting the content to be decoded
 and used based on the description of the de-
 fault usage-right information when the content
 includes the information indicating association
 with the default usage-right information.

14. A computer program according to Claim 13, where-
 in the content which is permitted for use based on
 the default usage-right information is provided for
 the purpose of sampling, and

said control step further includes a step of de-
 termining whether or not the content includes a
 flag indicating sample content, and permitting
 playback of the content according to a determi-
 nation result.

15. A computer program according to Claim 13, where-
 in the computer program further includes:

a sending step of sending a service registration request; and
a receiving step of receiving the default usage-right information sent from a license server in response to the registration request.

5

16. A computer program according to Claim 15, wherein the computer program further includes a step of receiving key information necessary for decoding the content.

10

17. A computer program for performing an information process for issuing a usage right having usage rules of encrypted content, said computer program including:

15

a receiving step of receiving a registration request; and
a sending step of sending key information and default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content.

20

18. A computer program according to Claim 17, wherein the content which is permitted for use based on the default usage-right information is provided for the purpose of sampling, and

25

the default usage-right information includes a description indicating that playback of the content is permitted when the content includes a flag indicating sample content.

30

19. A content usage management system including a content using apparatus for decoding and using encrypted content, and a usage-right issuing apparatus for issuing a usage right having usage rules of the encrypted content, wherein said content using apparatus comprises:

35

40

sending means for sending a service registration request; and
receiving means for receiving default usage-right information sent from a license server in response to the registration request, and said usage-right issuing apparatus comprises: receiving means for receiving the registration request; and
sending means for sending key information and the default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content.

45

50

55

20. A content usage managing method for a content usage management system including a content using apparatus for decoding and using encrypted con-

tent, and a usage-right issuing apparatus for issuing a usage right having usage rules of the encrypted content, said content usage managing method comprising:

a registration-request sending step of sending a service registration request from the content using apparatus to the usage-right issuing apparatus;

a data sending step of, in the usage-right issuing apparatus, receiving the registration request and sending key information and default usage-right information in response to the registration request, the key information being necessary for decoding the encrypted content; and

a receiving step of, in the content using apparatus, receiving the default usage-right information.

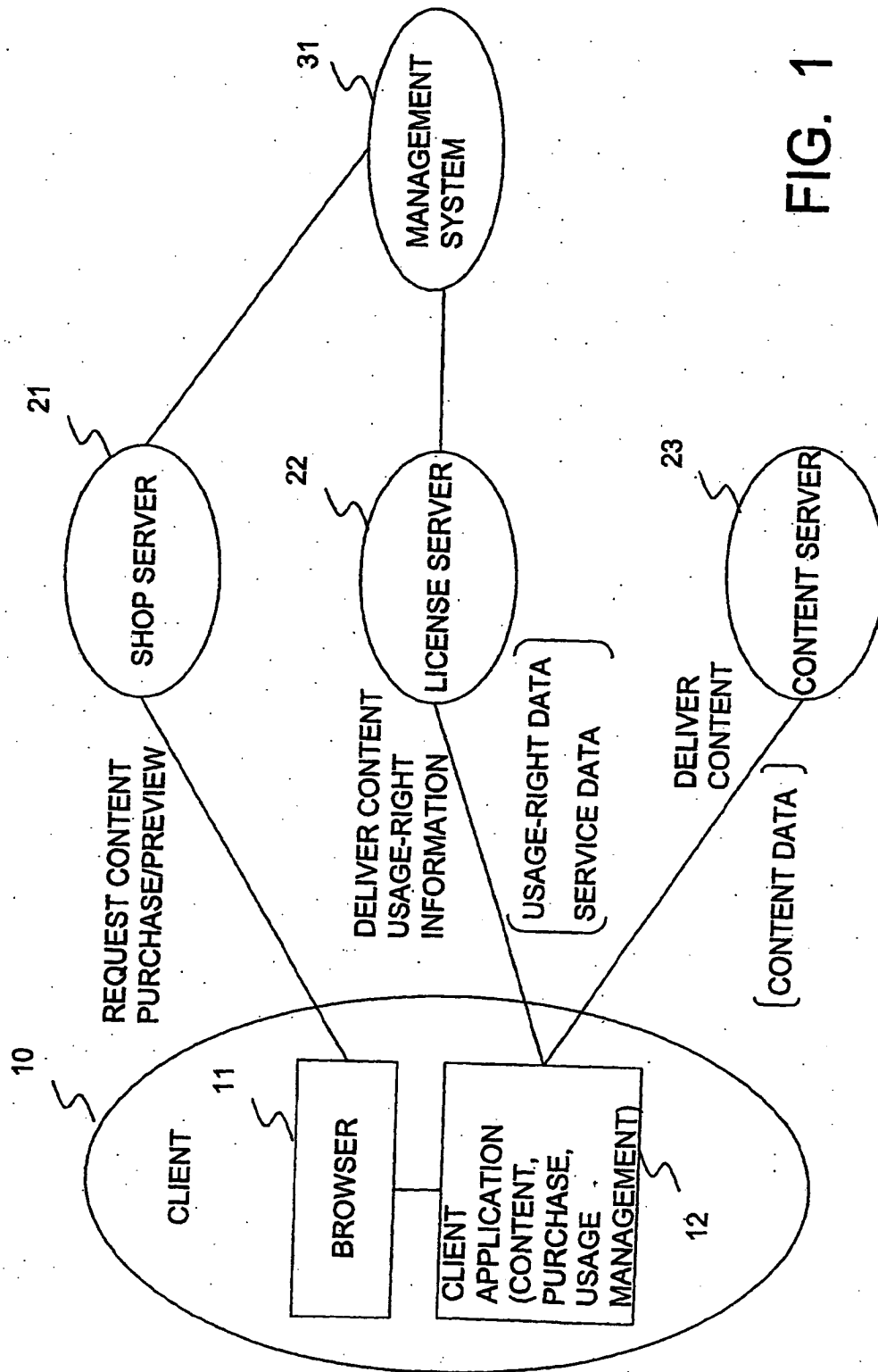


FIG. 1

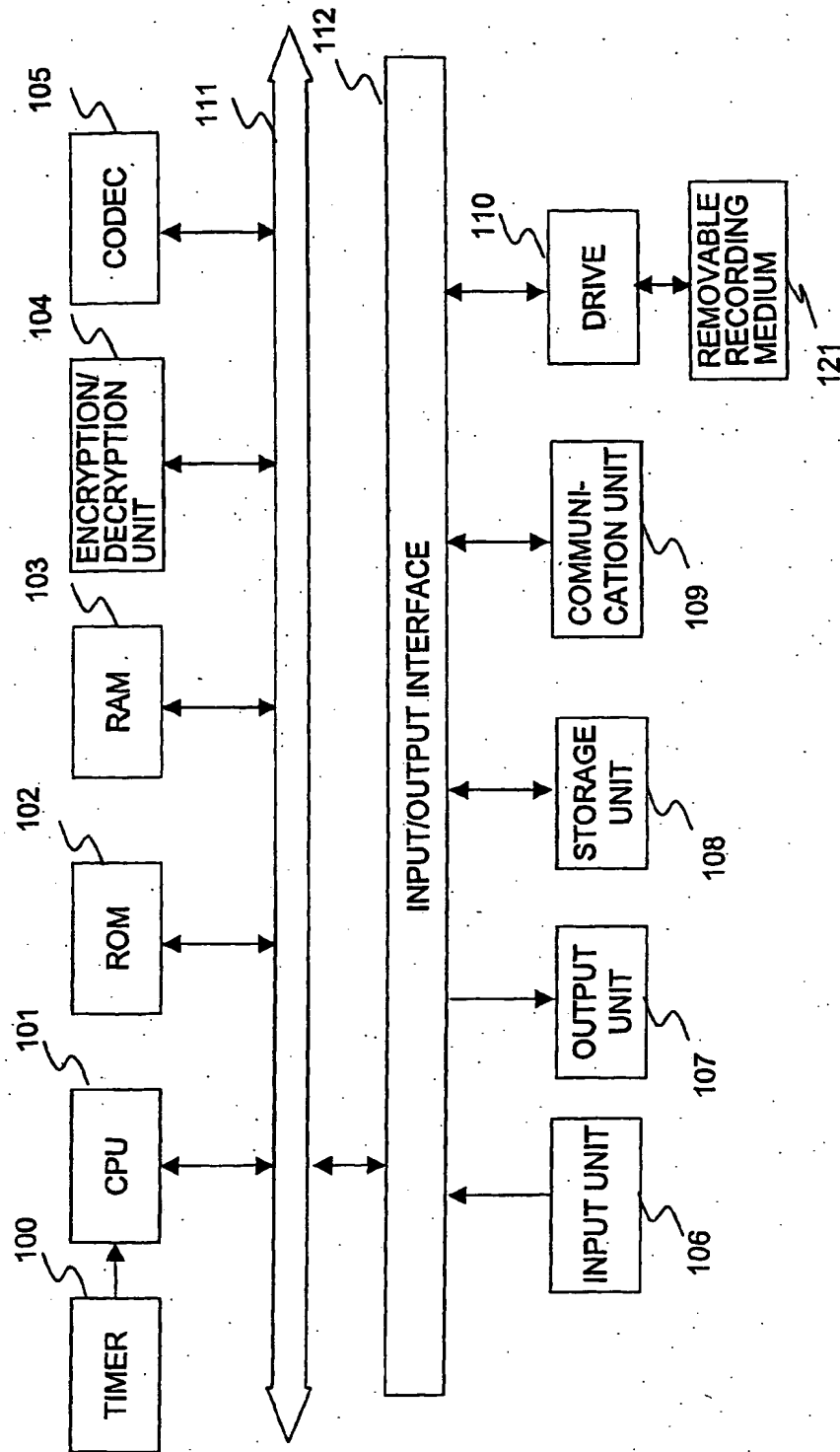
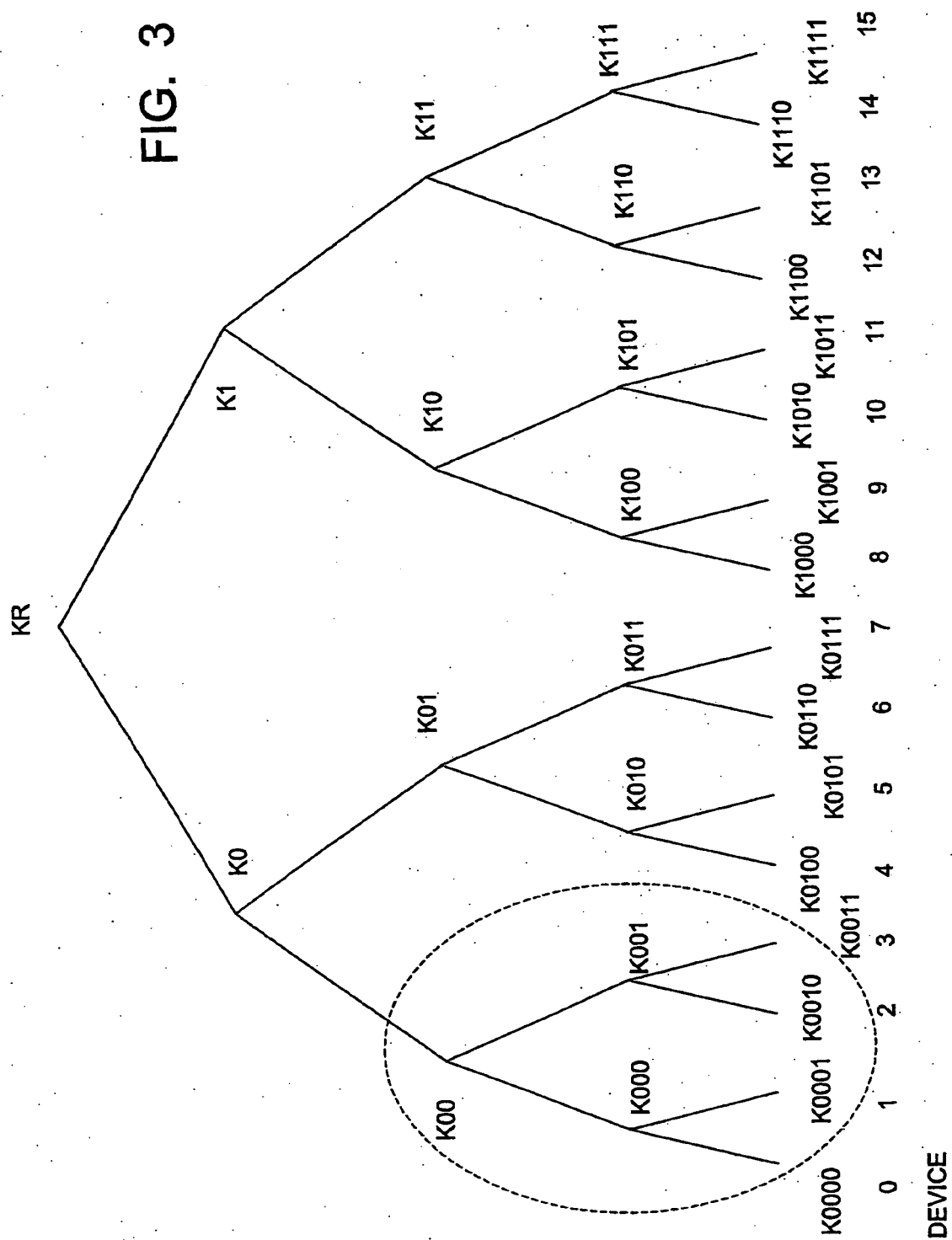


FIG. 2



(A) ENABLING KEY BLOCK (EKB) EXAMPLE 1

NODE KEYS AT VERSION t ARE SENT TO
DEVICES 0, 1, AND 2

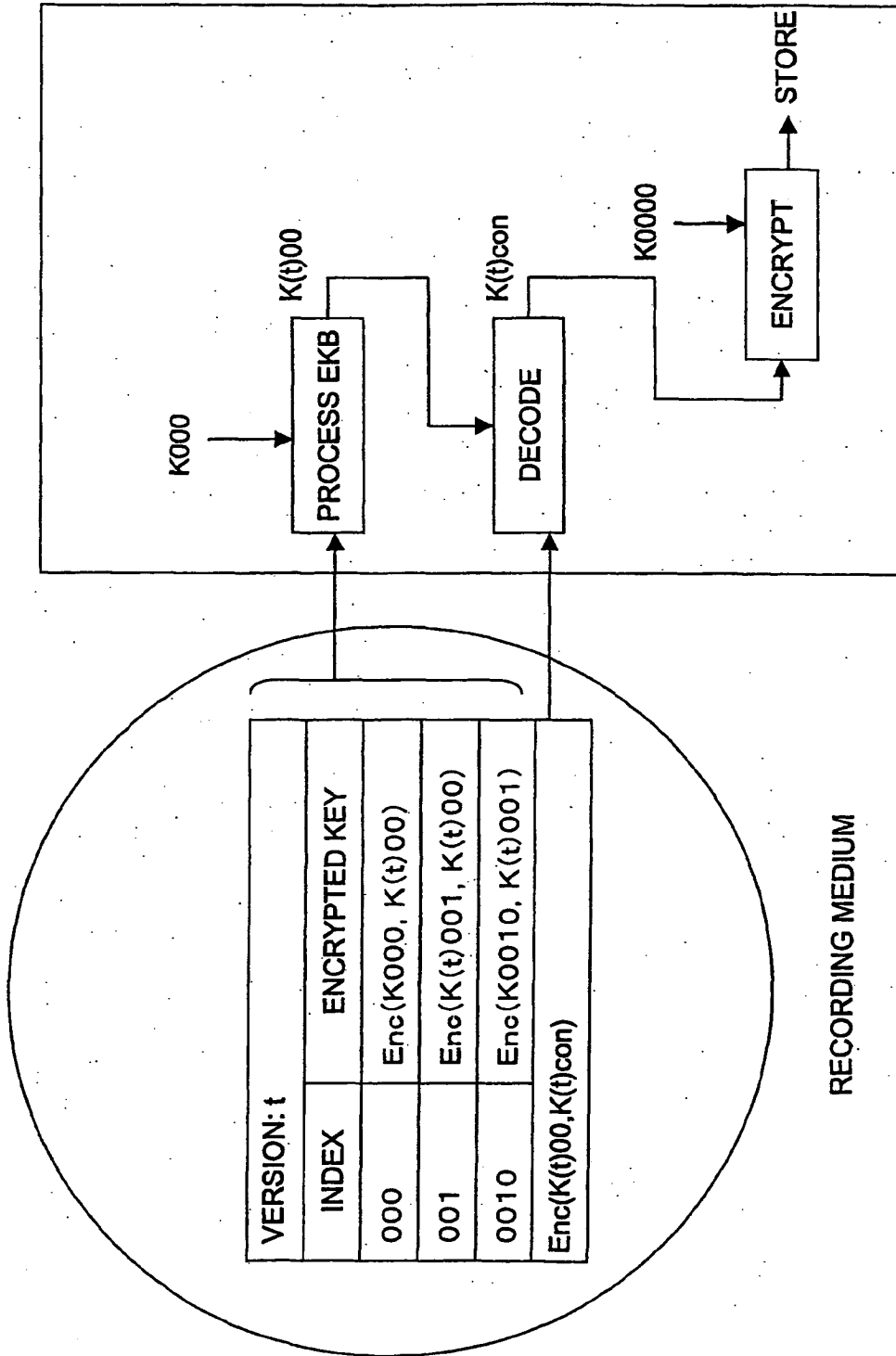
VERSION: t	
INDEX	ENCRYPTED KEY
0	$\text{Enc}(K(t)0, K(t)R)$
00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

(B) ENABLING KEY BLOCK (EKB) EXAMPLE 2

NODE KEYS AT VERSION t ARE SENT TO
DEVICES 0, 1, AND 2

VERSION: t	
INDEX	ENCRYPTED KEY
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

FIG. 4



DEVICE 0

FIG. 5

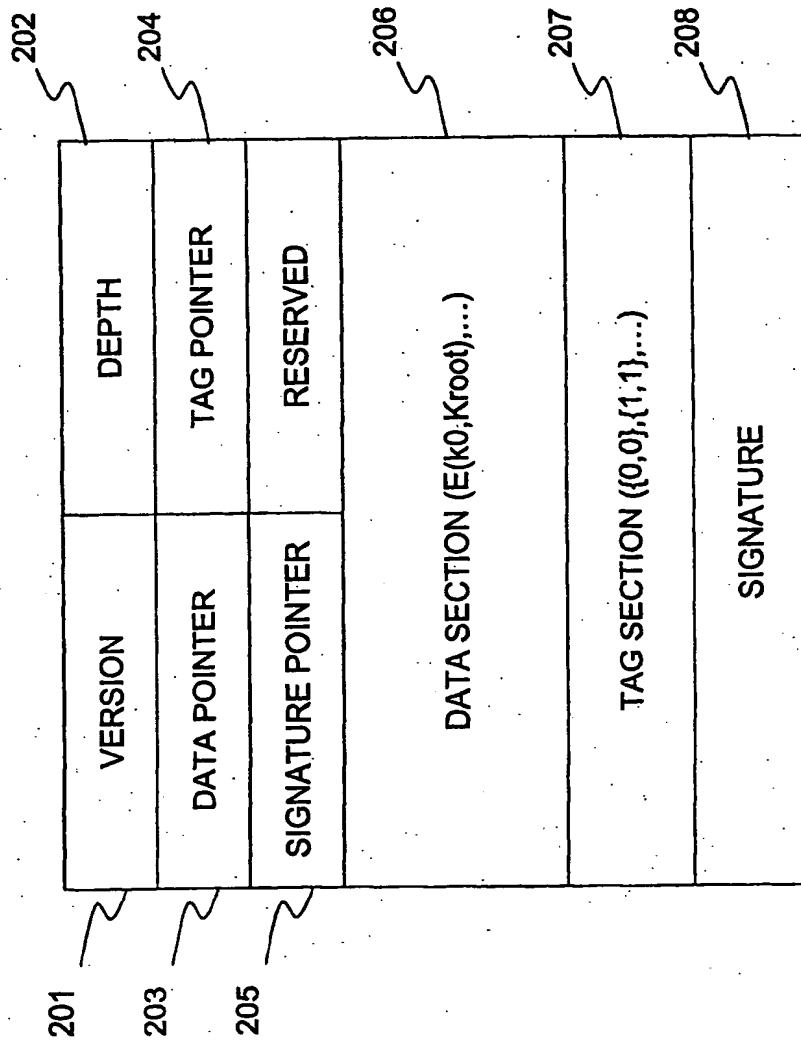
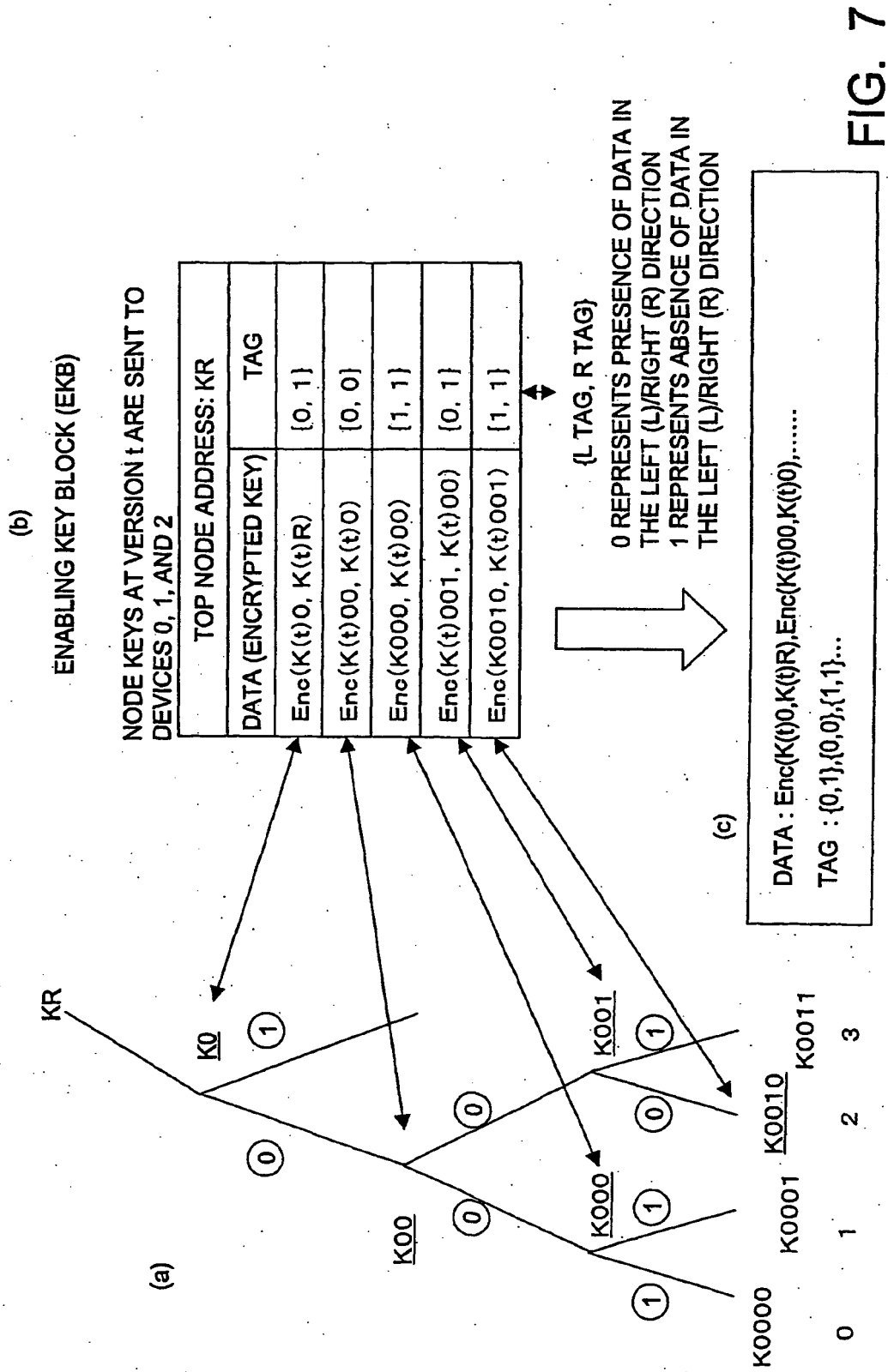


FIG. 6



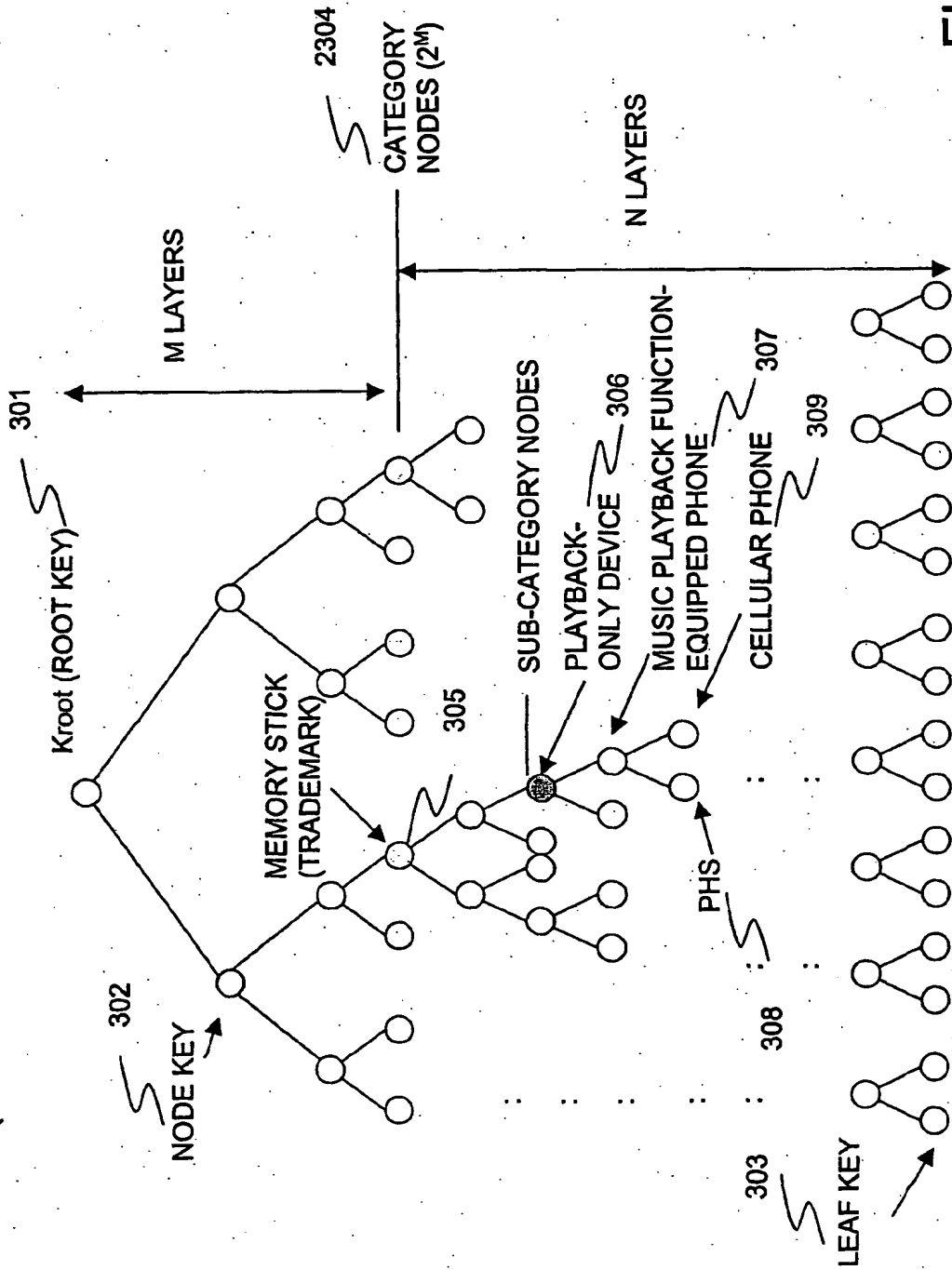


FIG. 8

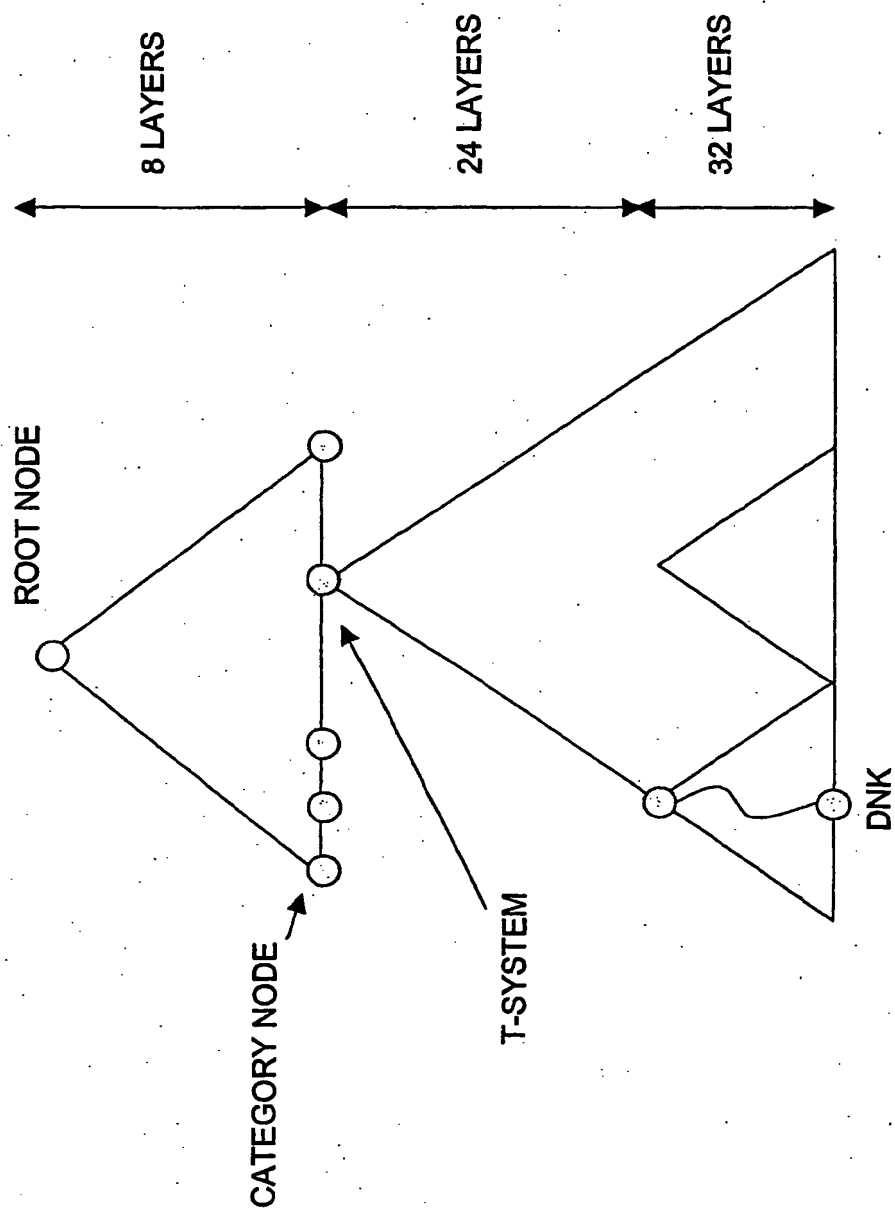


FIG. 9

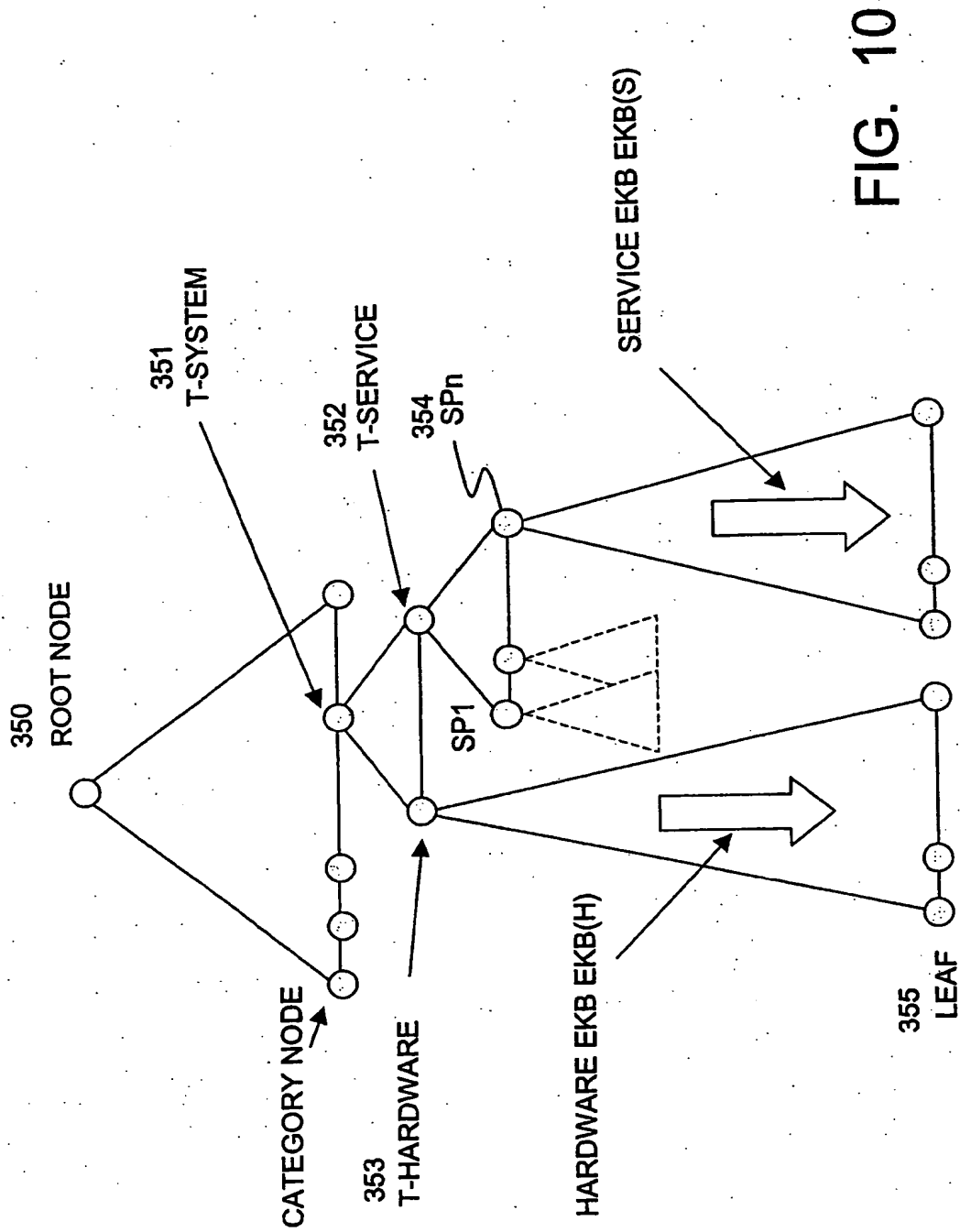


FIG. 10

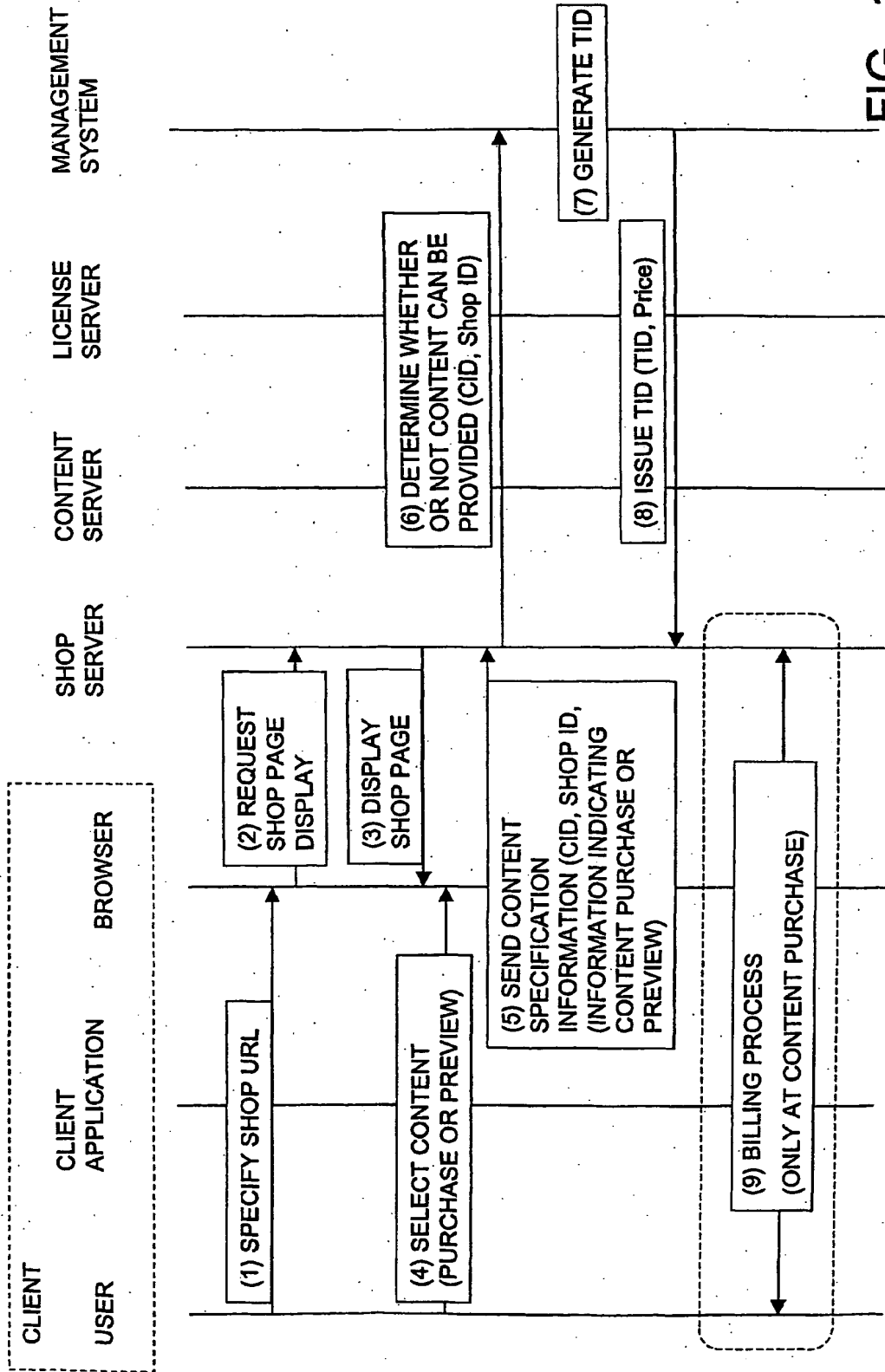


FIG. 11

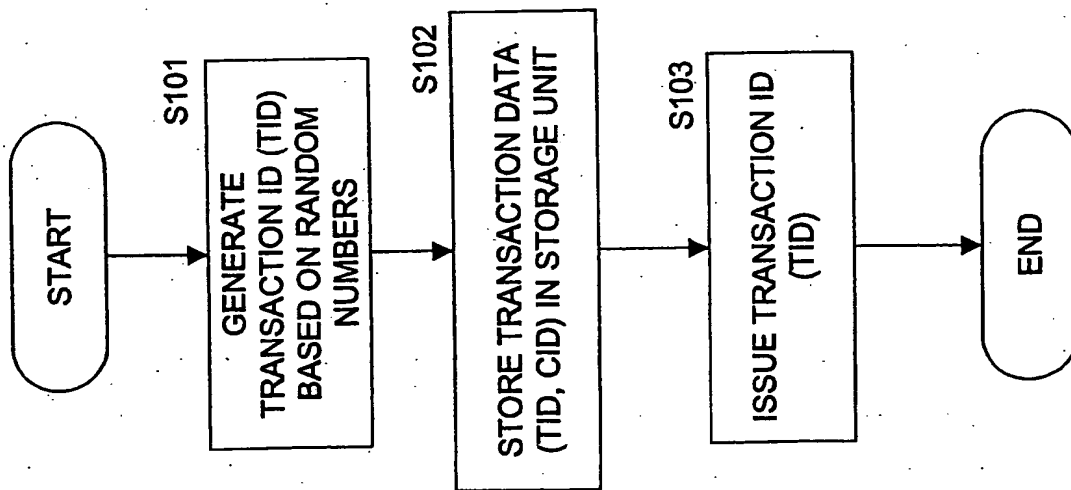


FIG. 12

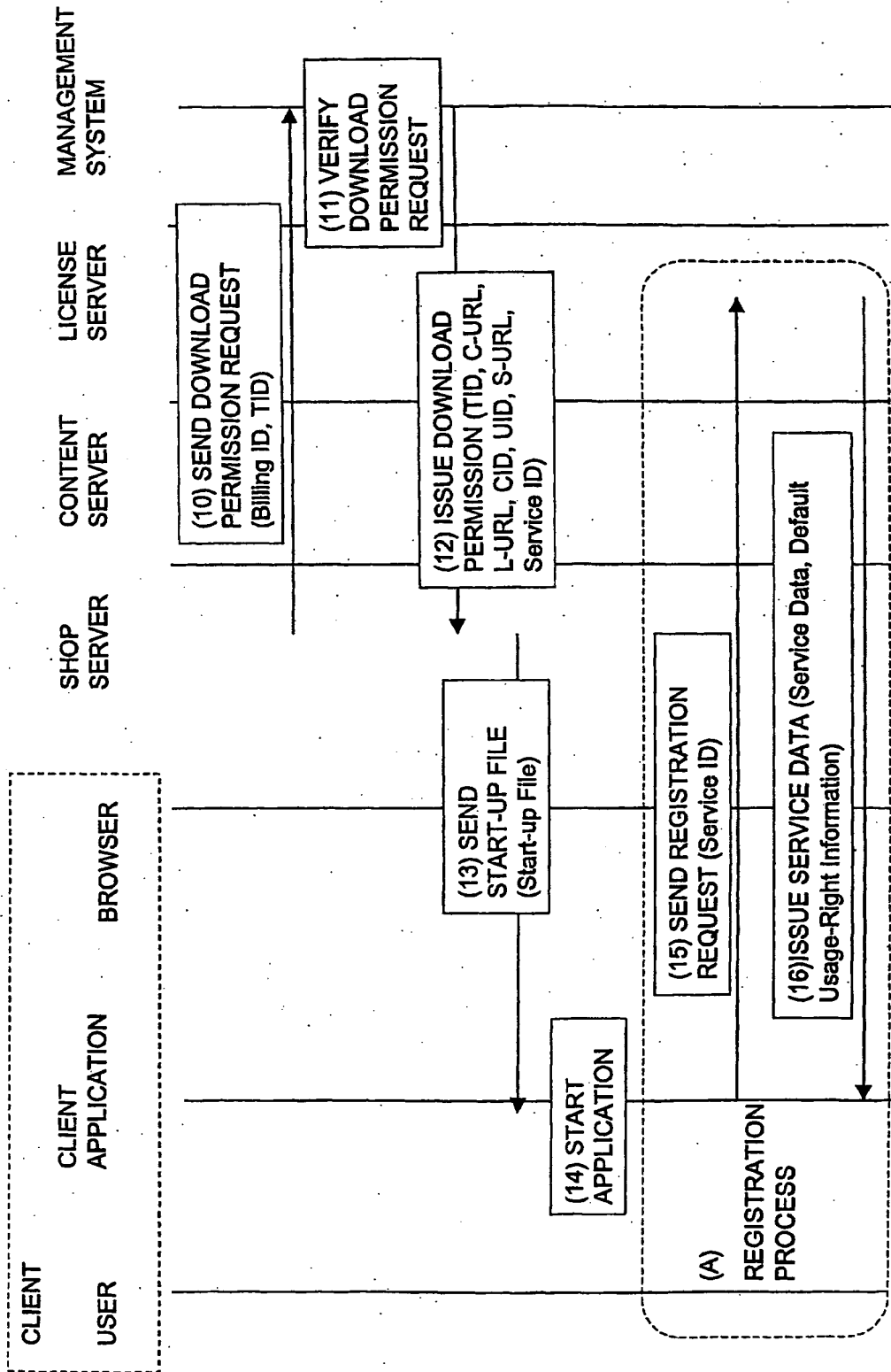


FIG. 13

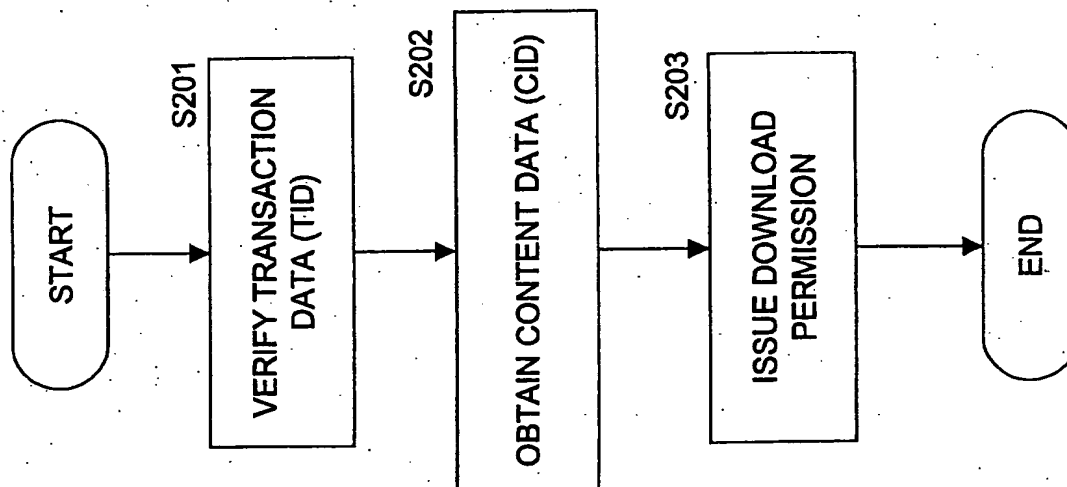


FIG. 14

360

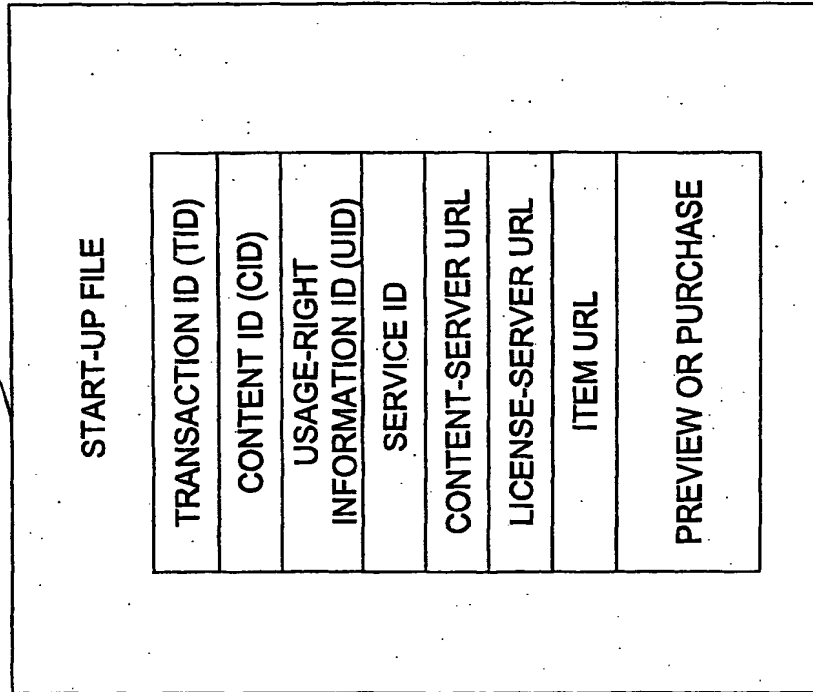


FIG. 15

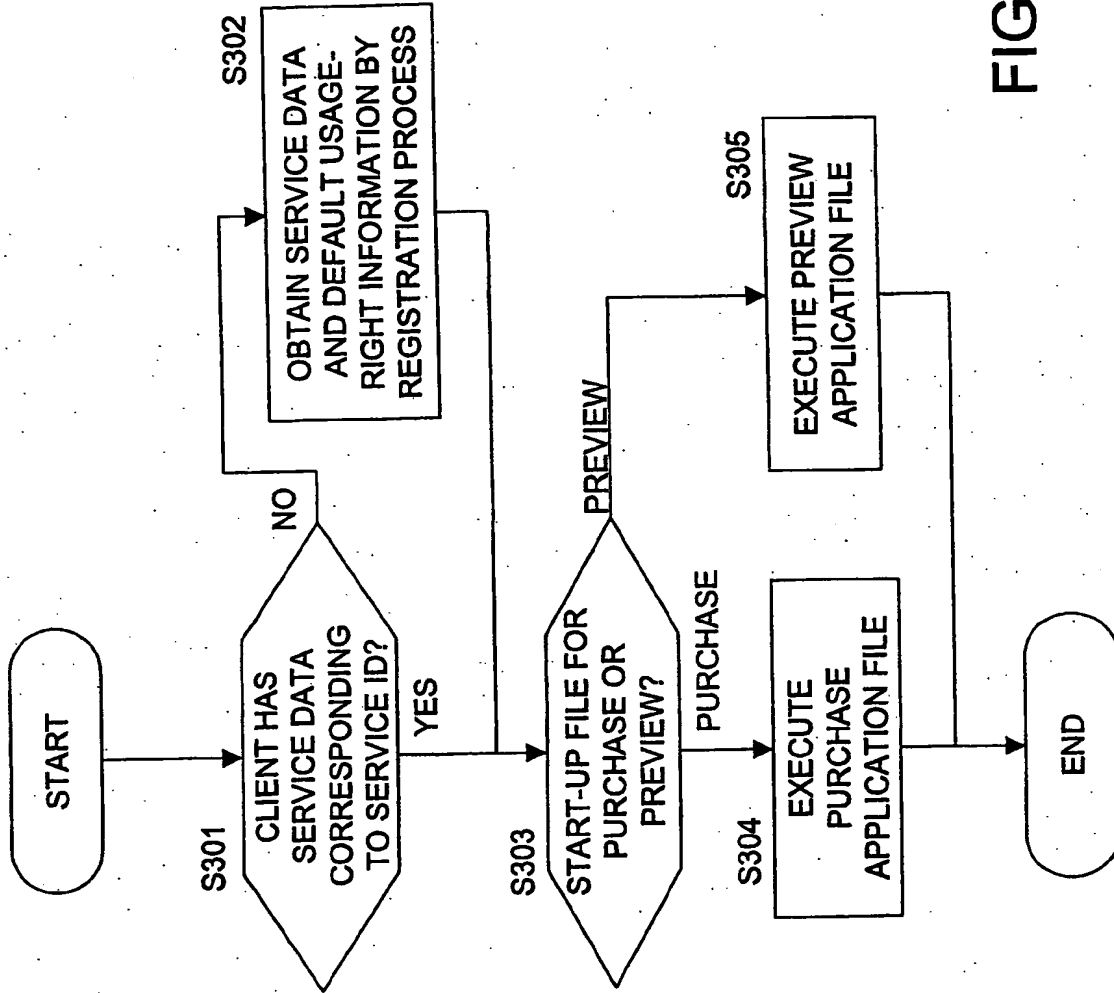


FIG. 16

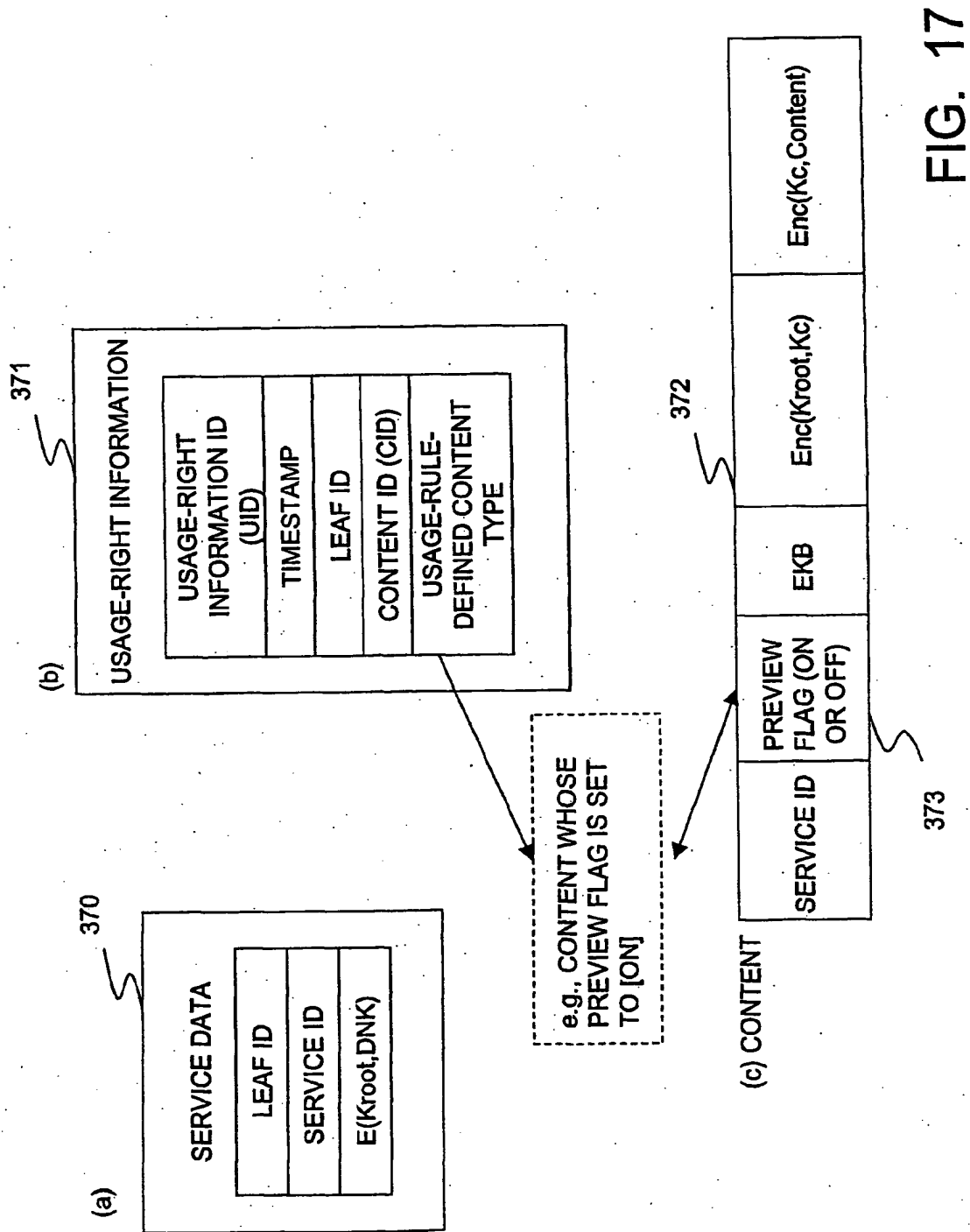


FIG. 17

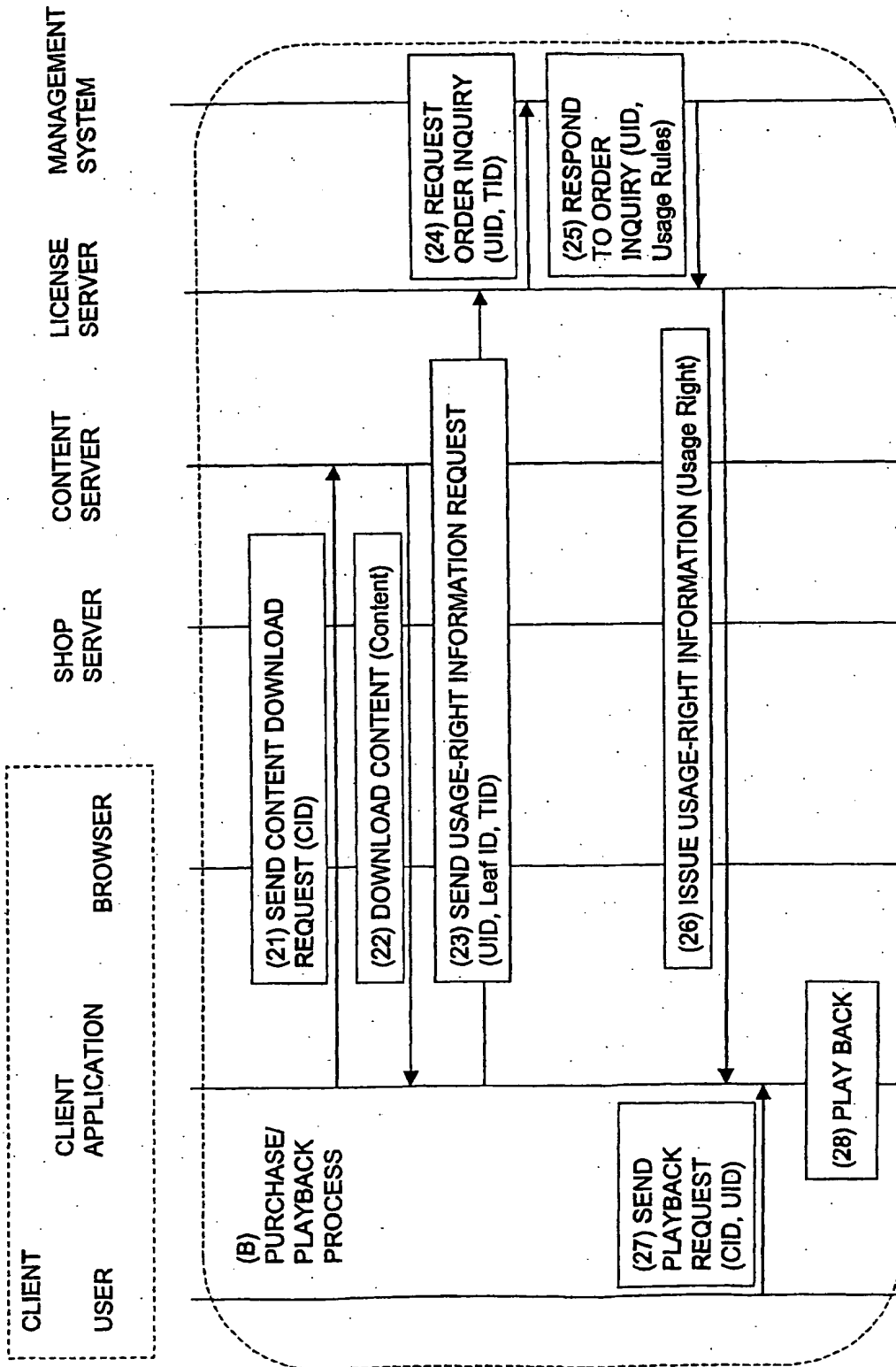


FIG. 18

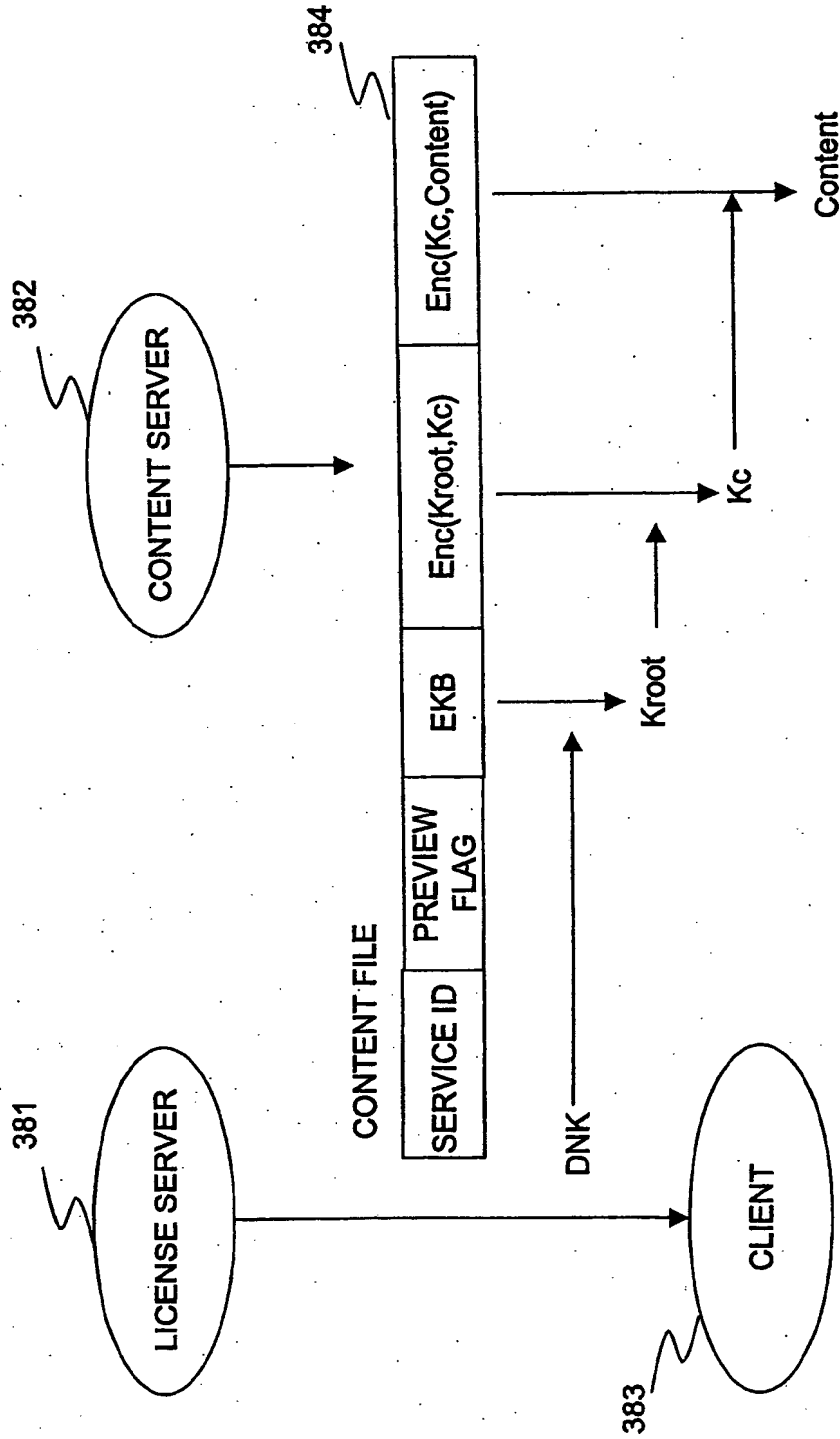
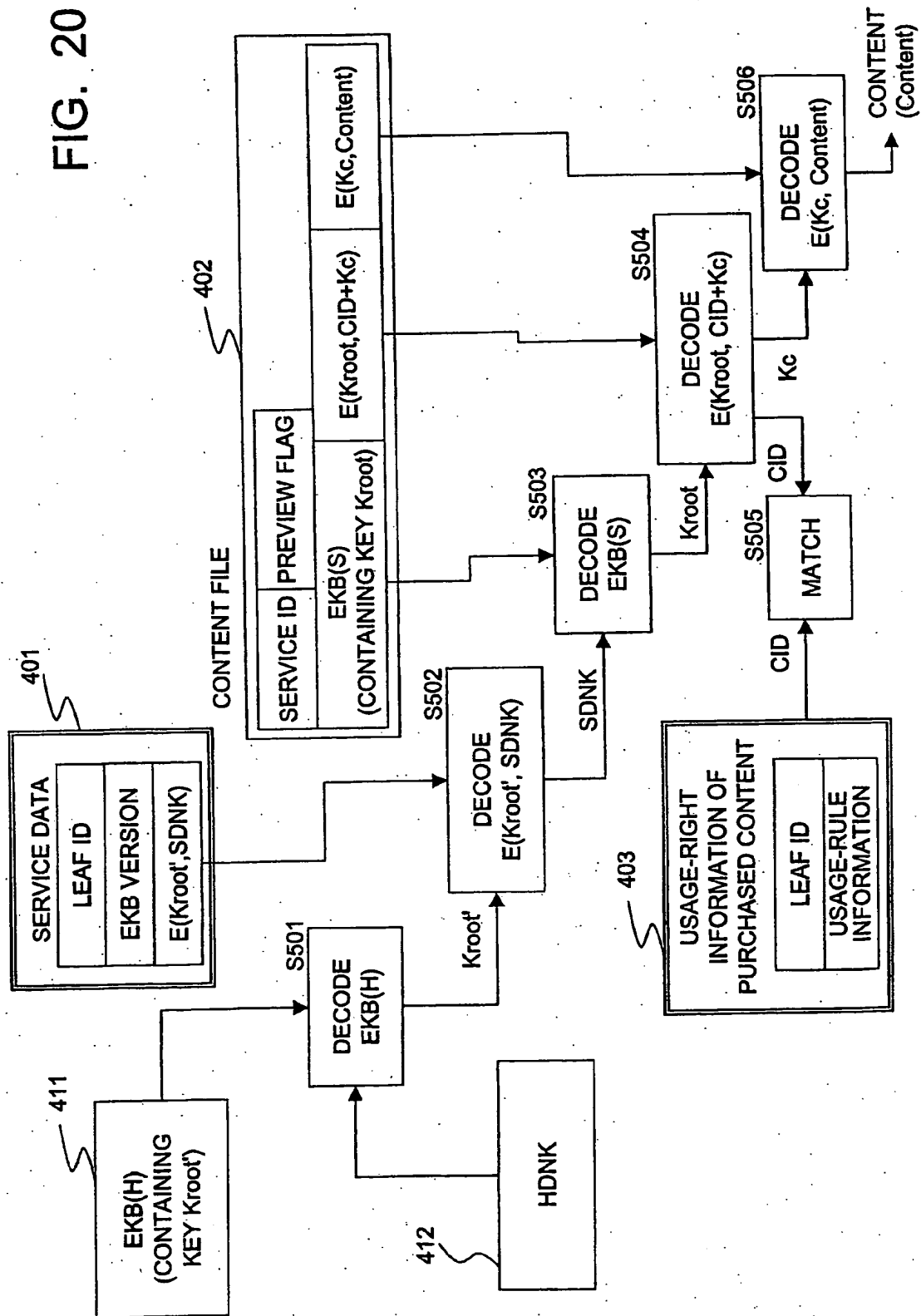


FIG. 19

FIG. 20



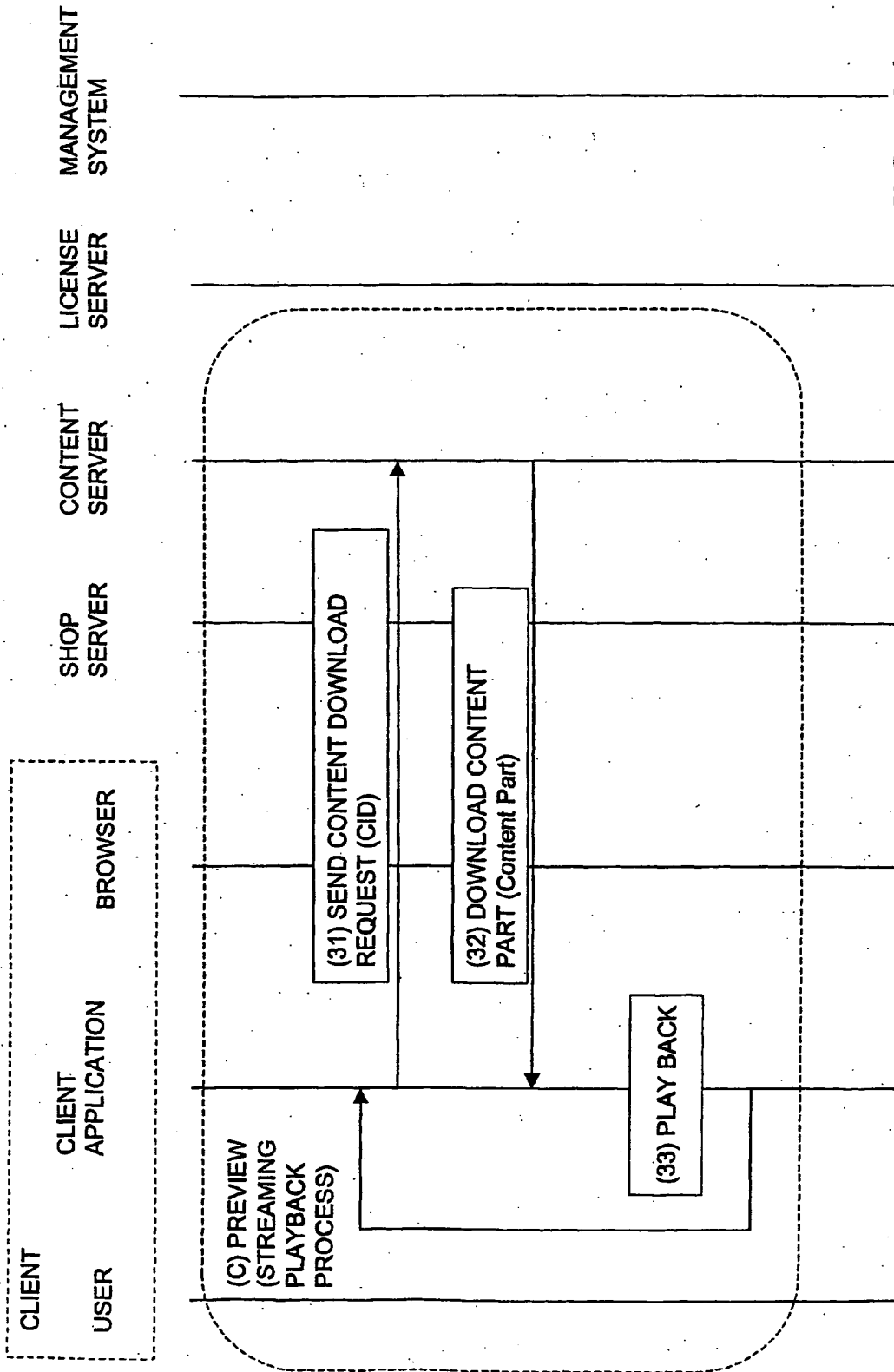


FIG. 21

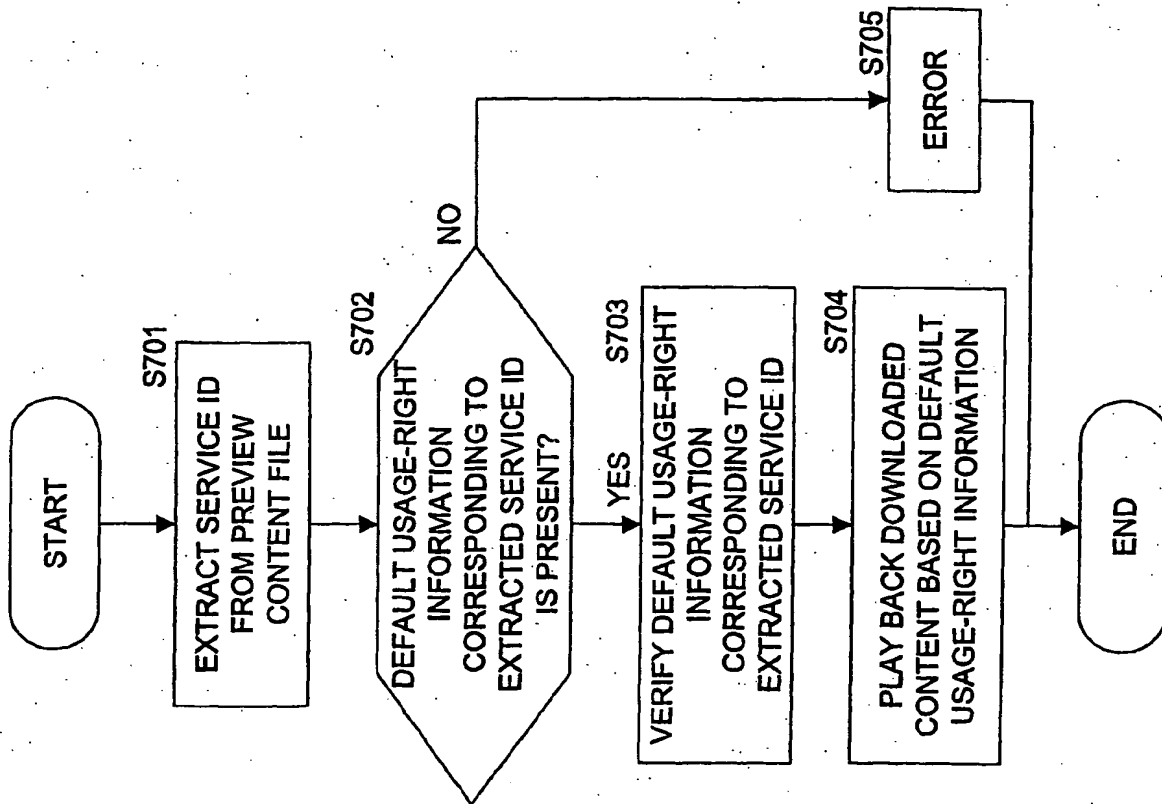


FIG. 22

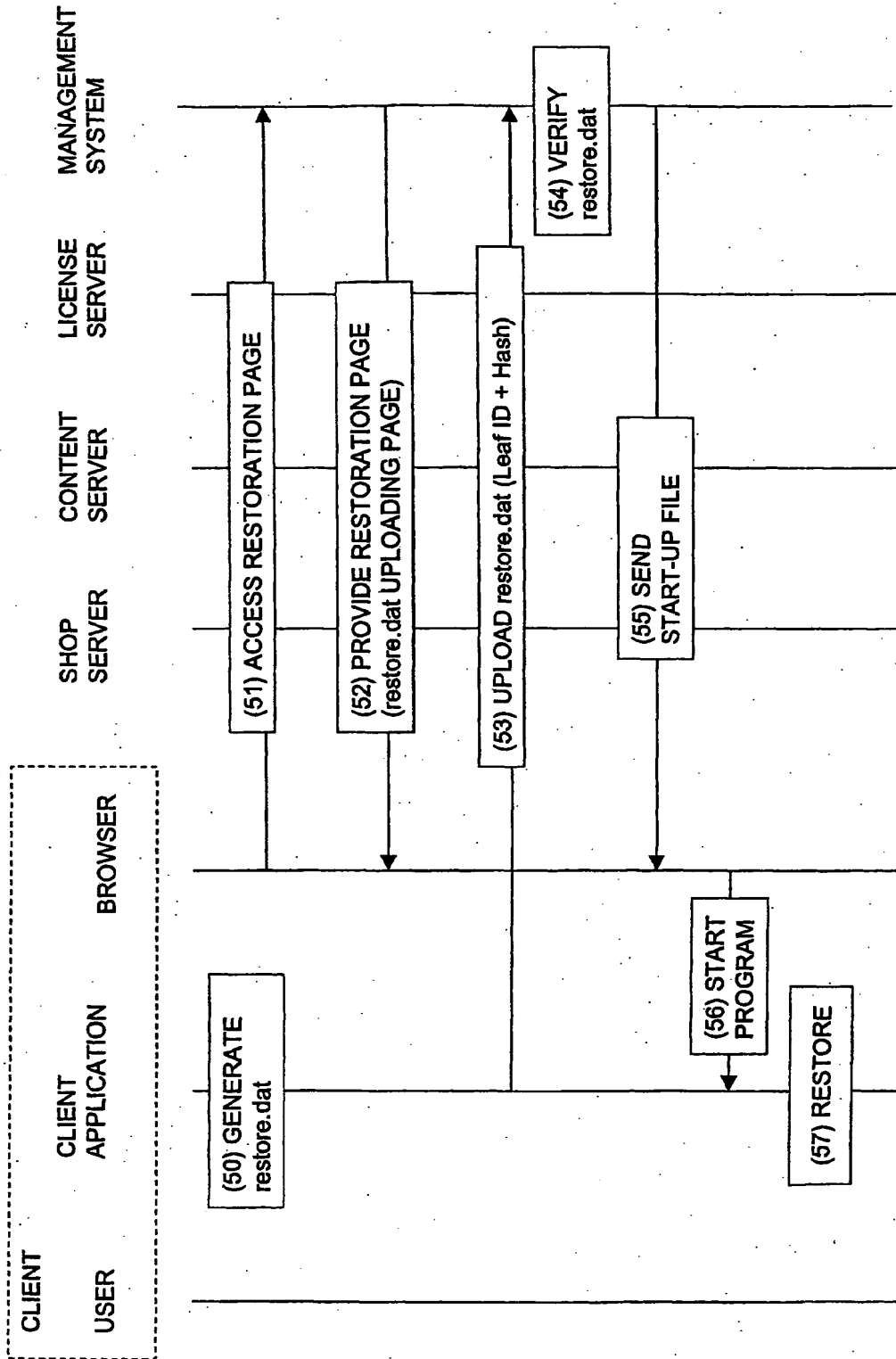


FIG. 23

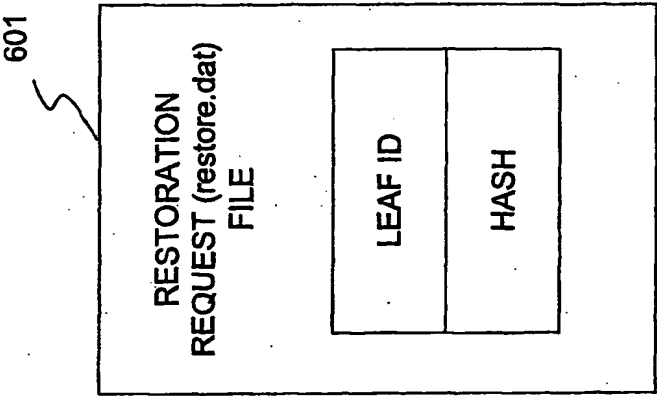
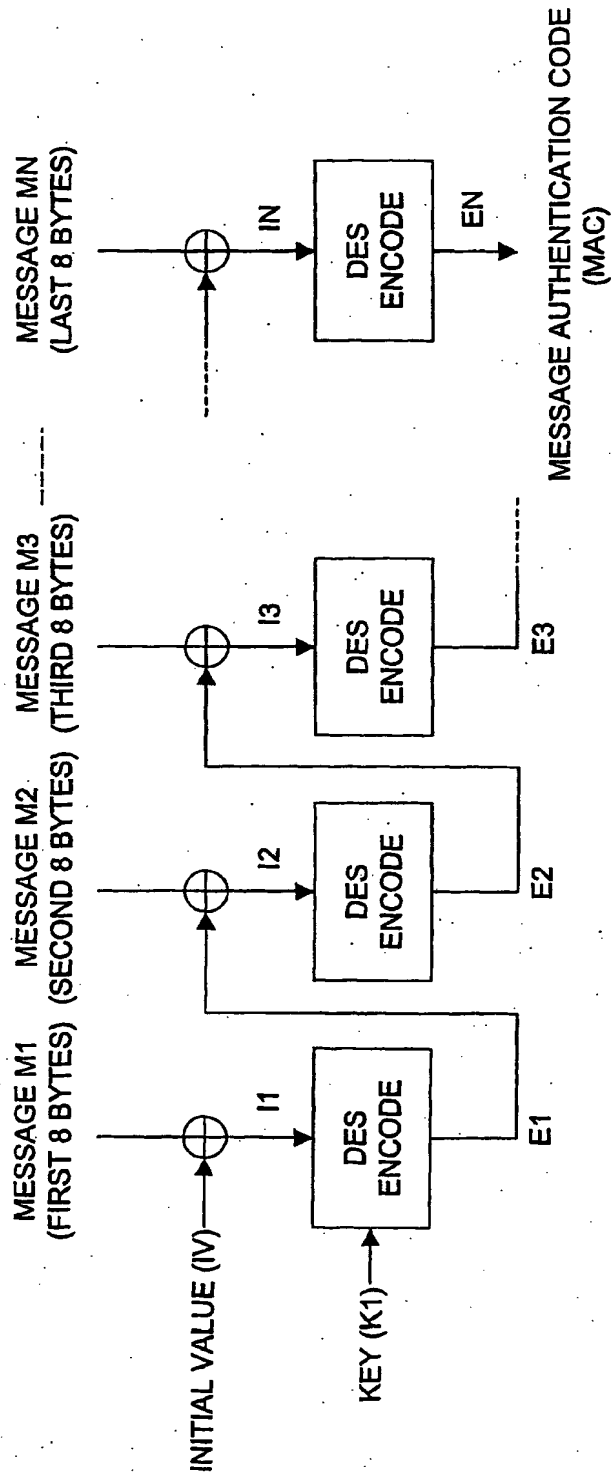


FIG. 24



\oplus : EXCLUSIVE-OR OPERATION (8-BYTE)

FIG. 25

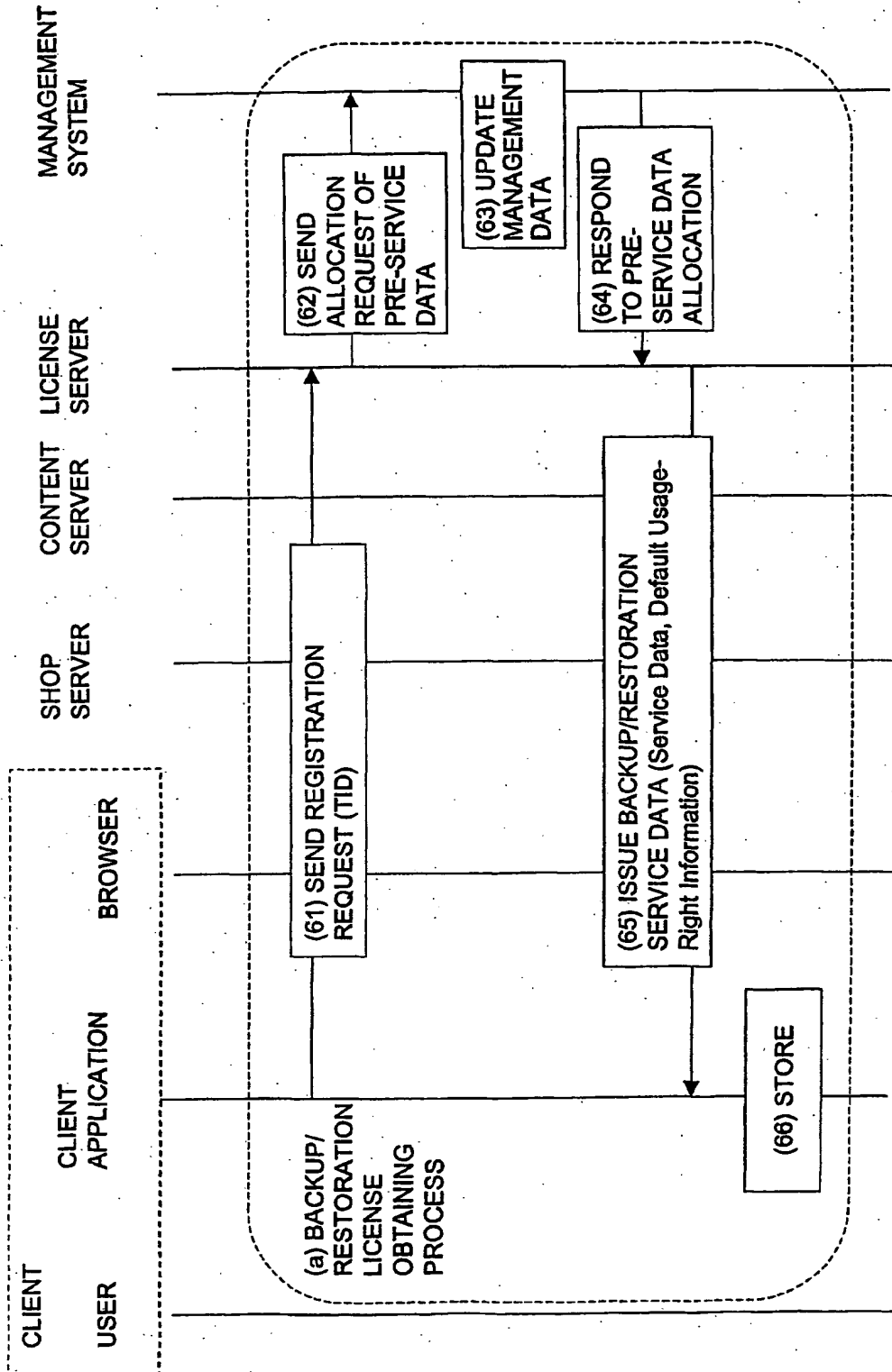


FIG. 26

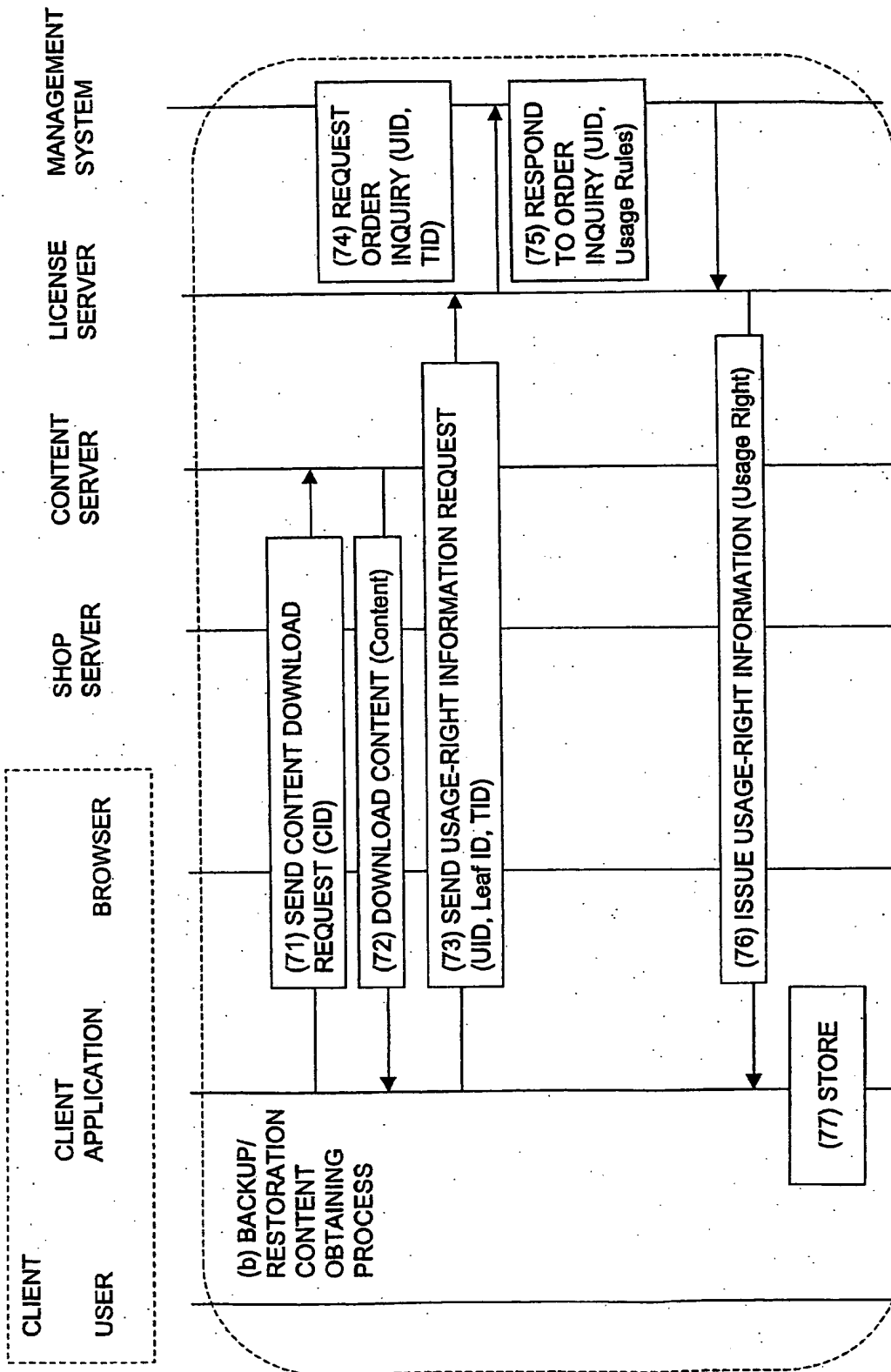


FIG. 27

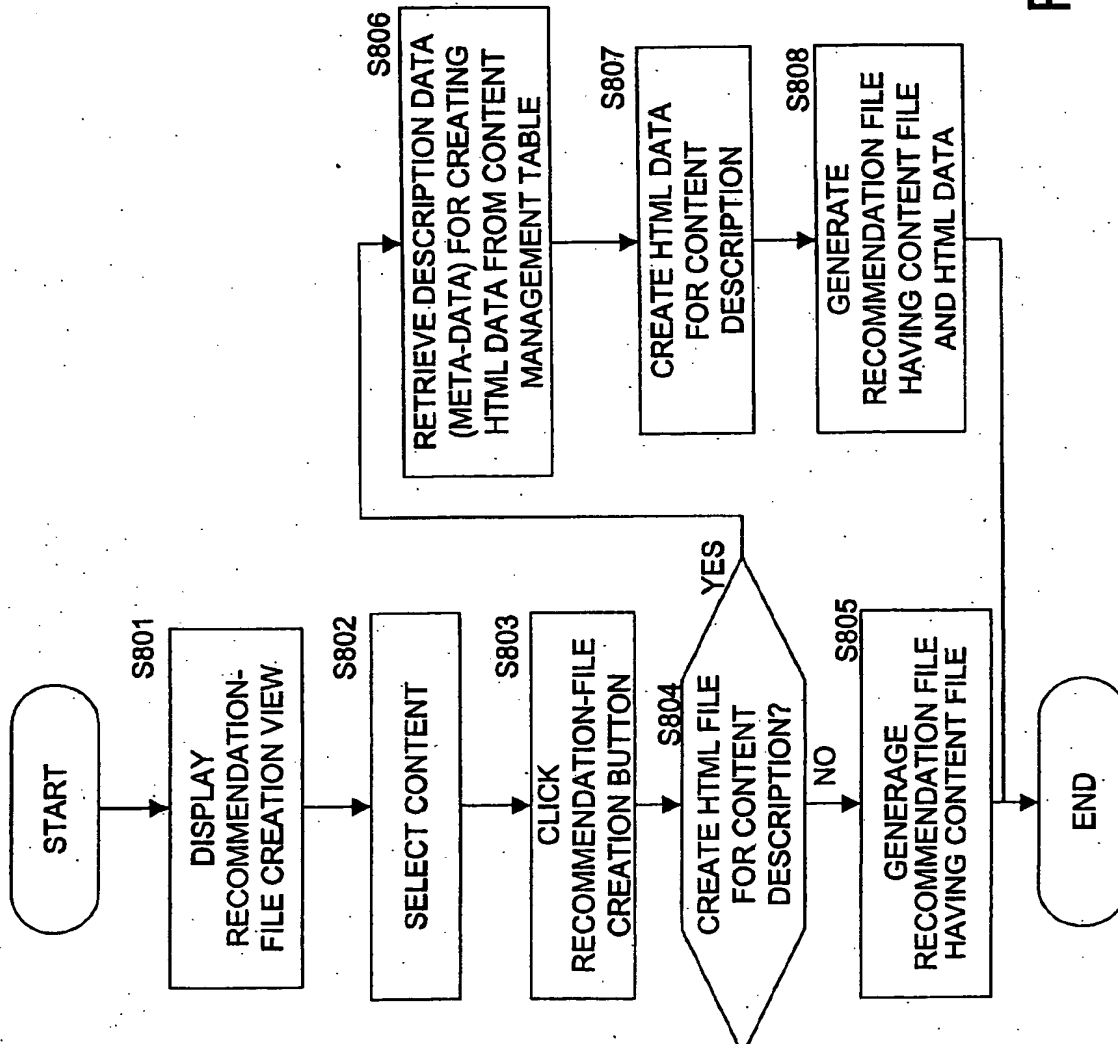


FIG. 28

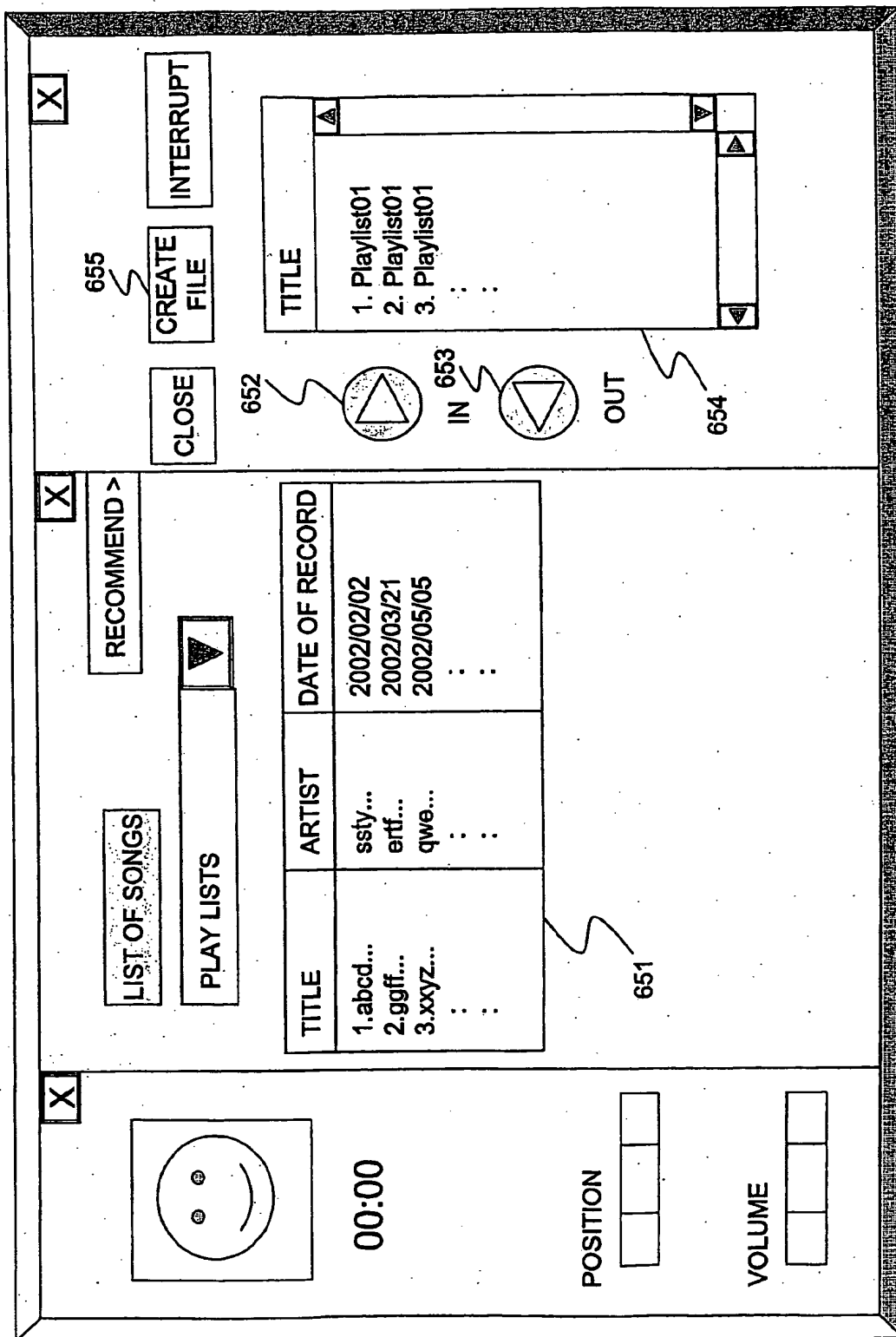


FIG. 29

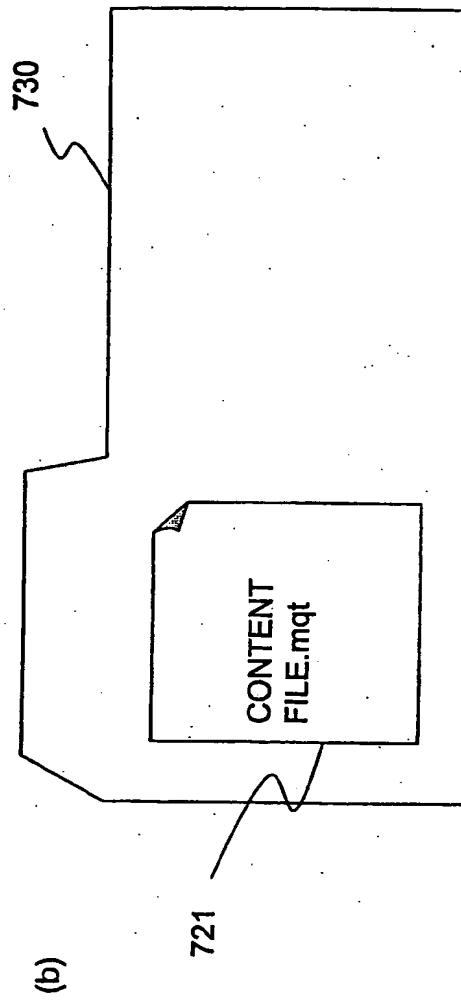
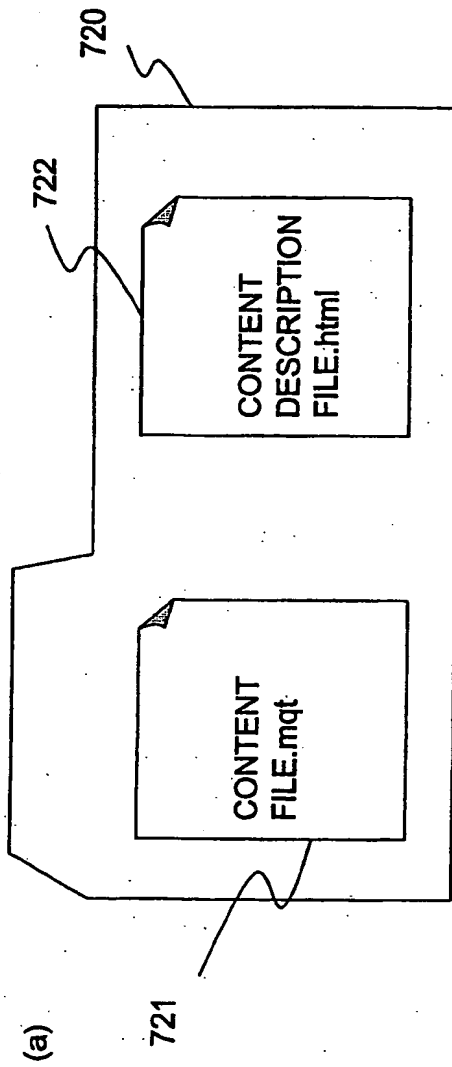


FIG. 30

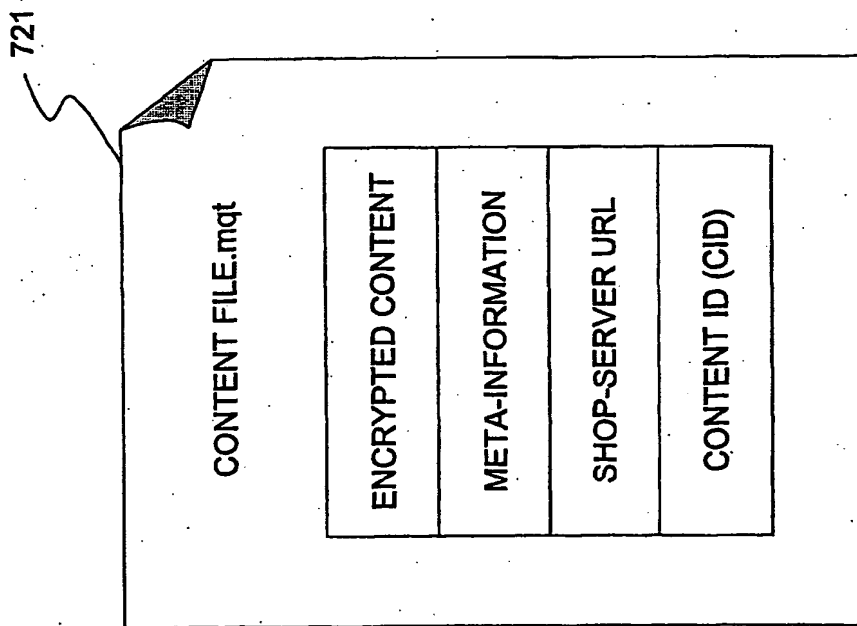


FIG. 31

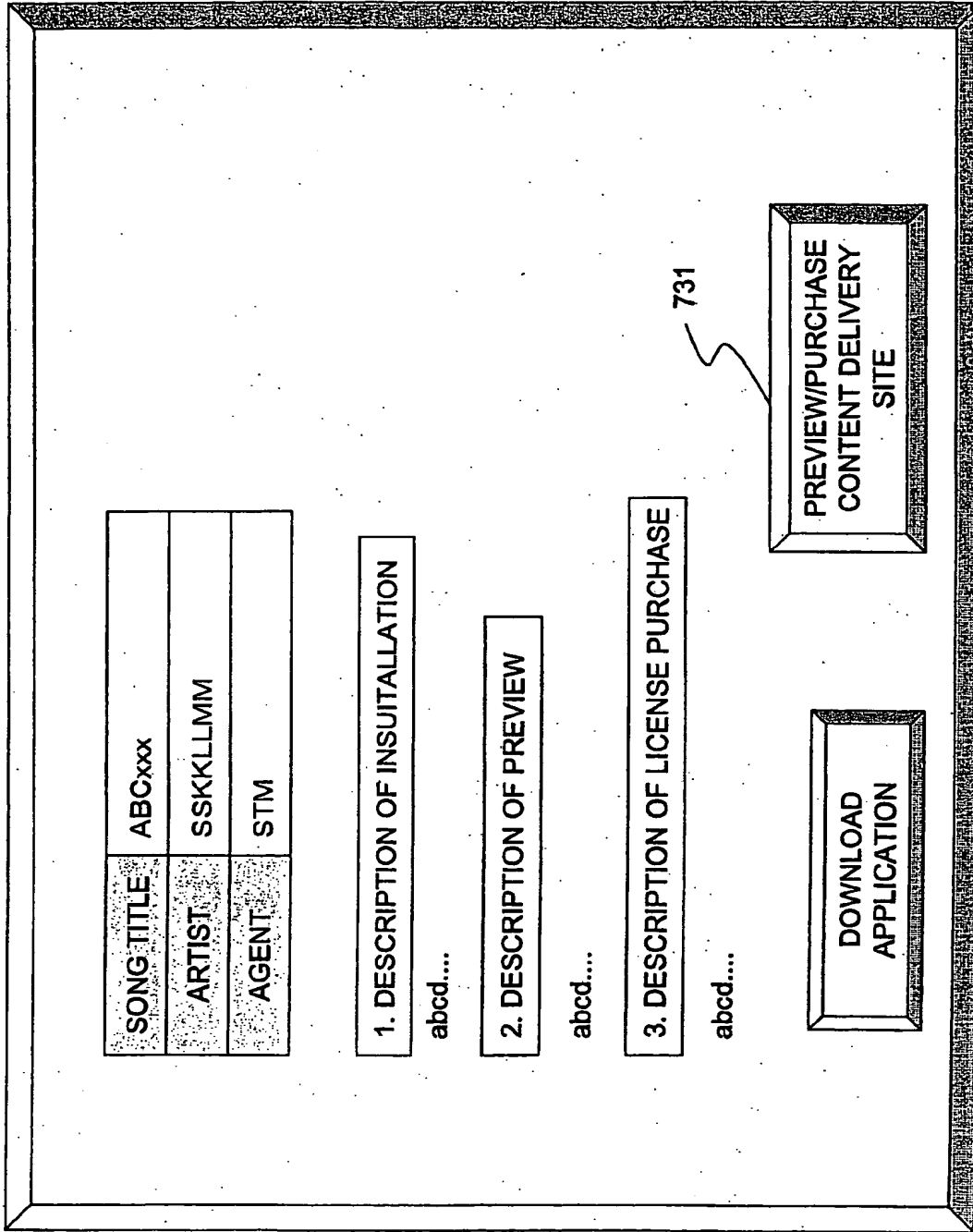


FIG. 32

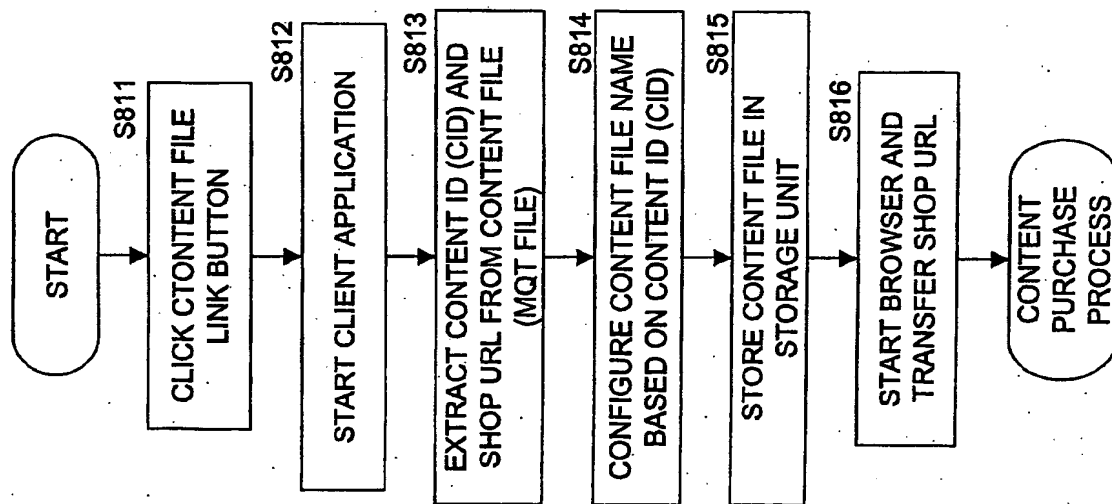


FIG. 33

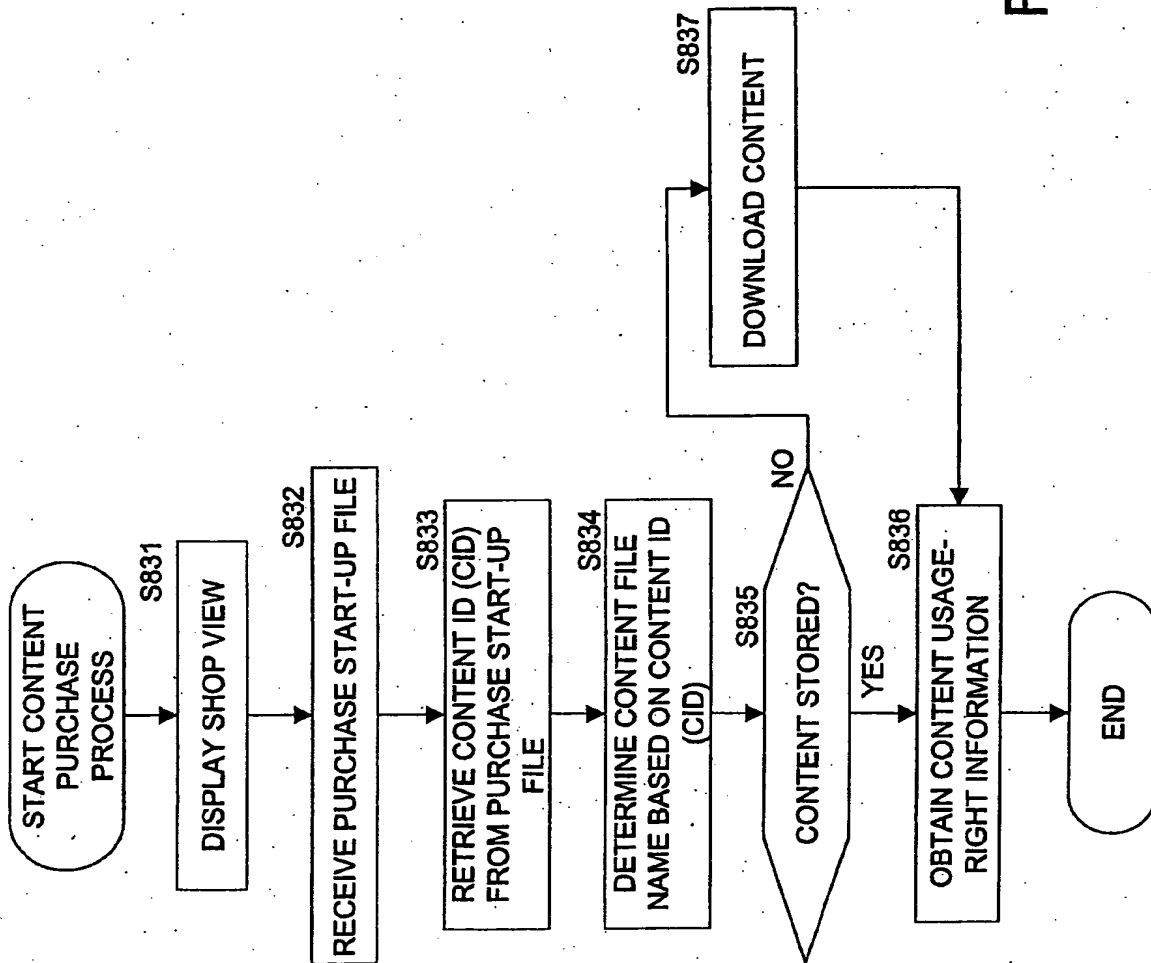


FIG. 34

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/08267

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl. ⁷ G06F12/14, H04L9/08, G06F17/60		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int.Cl. ⁷ G06F12/14, H04L9/08, G06F17/60		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2003 Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/44907 A1 (Microsoft Corp.), 21 June, 2001 (21.06.01), All pages; all drawings & WO 01/44908 A1 & WO 01/46783 A2	1,3-5,11, 17,19,20 2,6-10, 12-16,18
X	"Windows Media Rights Manager FAQ", [online], Microsoft Corporation, 2001, [retrieved on 2003- 09-04], Retrieved from the Internet: <URL: http:// web.archive.org/web/20010813233655/www.microsoft. com/japan/windows/windowsmedia/wm7/DRM/FAQ.asp? LNK=1>	1,3-5,11, 17,19,20 2,6-10, 12-15,18
Y		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 05 September, 2003 (05.09.03)		Date of mailing of the international search report 16 September, 2003 (16.09.03)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/08267

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Itaru HOSOMI, Masayuki NAKAE, Toshiharu ICHIYAMA, "Digital Joho Ryutsu Architecture MediaShell to sono Riyo-Kakin Seigyo", Information Processing Society of Japan Kenkyu Hokoku 98-EIP-2, Information Processing Society of Japan, 19 September, 1998 (19.09.98), Vol.98, No.85, pages 49 to 56	1,3-5,11, 17,19,20 2,6-10, 12-16,18
Y	JP 2000-293439 A (Fujitsu Ltd.), 20 October, 2000 (20.10.00), All pages; all drawings (Family: none)	1,3-5,11, 17,19,20 2,6-10, 12-16,18
Y	JP 8-272746 A (Xerox Corp.), 18 October, 1996 (18.10.96), All pages; all drawings & US 5634012 A & EP 715243 A1	2,6-10, 12-16,18
Y	JP 7-221751 A (Nippon Telegraph And Telephone Corp.), 18 August, 1995 (18.08.95), All pages; all drawings (Family: none)	2,6-10, 12-16,18
Y	JP 9-297682 A (NEC Corp.), 18 November, 1997 (18.11.97), All pages; all drawings (Family: none)	2,6-10, 12-16,18
Y	JP 2002-133147 A (Fujitsu Ltd.), 10 May, 2002 (10.05.02), All pages; all drawings (Family: none)	2,6-10, 12-16,18

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

THIS PAGE BLANK (USPTO)

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004 年 1 月 29 日 (29.01.2004)

PCT

(10) 国際公開番号
WO 2004/010307 A1

- (51) 国際特許分類: G06F 12/14, H04L 9/08, G06F 17/60
- (21) 国際出願番号: PCT/JP2003/008267
- (22) 国際出願日: 2003 年 6 月 30 日 (30.06.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-213700 2002 年 7 月 23 日 (23.07.2002) JP
- (71) 出願人(米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 北谷 義道 (KI-TAYA, Yoshimichi) [JP/JP]; 〒141-0001 東京都品川区

北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 栗屋 志伸 (KURIYA, Shinobu) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭, 外 (MIYATA, Masaaki et al.); 〒104-0041 東京都中央区新富一丁目 1 番 7 号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国(国内): CN, KR, US.

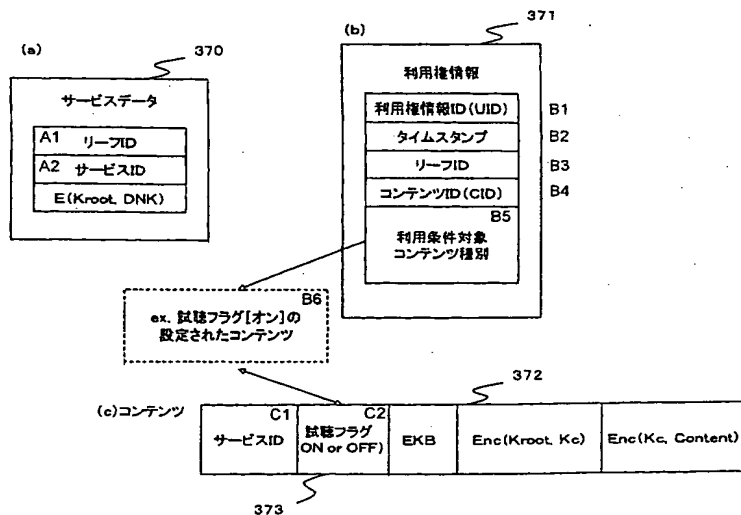
(84) 指定国(広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 情報処理装置、および情報処理方法、並びにコンピュータ・プログラム



370...SERVICE DATA
A1...LEAF ID
A2...SERVICE ID
371...USAGE RIGHT INFORMATION
B1...USAGE RIGHT INFORMATION ID (UID)
B2...TIME STAMP
B3...LEAF ID
B4...CONTENT ID (CID)
B5...CONTENT TYPE OF USAGE CONDITION
B6...ex. CONTENT IN WHICH TEST LISTENING FLAG IS SET TO "ON"
(C)...CONTENT
C1...SERVICE ID
C2...TEST LISTENING FLAG ON or OFF

(57) Abstract: A device and a method for realizing an improved processing for content test listening in content use based on content usage right information. Upon registration on a license server, a client acquires a default usage right and upon test listening not requiring content purchase processing, it is judged whether content reproduction is enabled according to the default usage right information. A client allowed to perform test listening is limited to a client who has performed registration on the license server and has default usage right information. Thus, it is possible to prevent flood of test listening data out of order.

(57) 要約: コンテンツの利用権情報に基づくコンテンツ利用構成において、コンテンツ試験における改良された処理を実現する装置、方法を提供する。クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報 (Default Usage Right) を取得し、コンテンツの購入処理を伴わない試験処理の際にデフォルト利用権情報に基づいてコンテンツ再生の可否を判定する。試験が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試験データが無秩序に氾濫してしまうことが防止される。

WO 2004/010307 A1



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

情報処理装置、および情報処理方法、並びにコンピュータ・プログラム

5 技術分野

本発明は、情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。特に、コンテンツの再生等の利用時におけるコンテンツ利用権の確認を実現し、また、コンテンツの試聴、試写処理を可能としてユーザに対するフレキシブルなコンテンツ利用態様を実現した情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。

背景技術

15

昨今、音楽データ、ゲームプログラム、画像データ等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の、インターネット等のネットワーク、あるいは、メモ리카ード、HD、DVD、CD等の流通可能な記憶媒体を介した流通が盛んになっている。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、記録再生器、再生専用器、あるいはゲーム機器内の記憶手段、例えばHD、フラッシュメモリを有するカード型記憶装置、CD、DVD等に格納され、再生処理が実行される。

25 記録再生装置、ゲーム機器、PC等の情報機器には、コンテンツをネットワークから受信するためのインタフェース、あるいはメモ리카ード、HD、DVD、CD等にアクセスするためのインタフェースを有し、コンテンツの再生に必要な制御手段、プログラム、データのメモリ領域として使用されるRAM、ROM等を有する。

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用される記録再生装置、ゲーム機器、P C等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により、例えば内蔵、あるいは着脱自在の記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われなくようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

また、コンテンツと、コンテンツを利用する利用権とを独立に管理し、ユーザに提供する構成が提案されている。この構成において、ユーザは、例えば暗号化されたコンテンツを取得し、さらに、利用権データを購入することにより、利用権データから取得可能な鍵データ等に基づいて、暗号化コンテンツの復号用の鍵（コンテンツ鍵）を取得して、コンテンツを利用する。

利用権データには、ユーザのコンテンツ利用許可態様の設定情報が格納され、その許可情報において許された範囲でのコンテンツの利用が可能となるといったシステムが提案されている。

発明の開示

このように、コンテンツとコンテンツ利用権とを独立に管理し、ユーザに提供するシステムにおいては、コンテンツの利用、例えば音楽デー

タ、画像データの再生、または配信、あるいはダウンロード処理に際して、利用権データのチェックが実行される。

このような構成において、利用権チェックの際、ユーザがコンテンツの利用をする権利がないと判定された場合には、コンテンツの再生、配信、ダウンロードが実行されないことになる。

しかしながら、コンテンツの購入以前に、コンテンツの一部等を試聴、あるいは試写を行なって、コンテンツの内容を確認した上で、コンテンツの購入を行ないたいという要望があるのも事実であり、このような場合に、通常の利用権のチェック処理を行なえば、利用権が無いとの判定によって、コンテンツ再生等の処理が拒否されてしまうことになる。

このような状況に対応するためには、利用権を全く考慮しないフリーのサンプルデータをユーザに対して配布する構成とすることも可能であるが、ほとんどのコンテンツには著作権者の著作権、頒布者の頒布権が存在する。従って、コンテンツの一部であっても、コンテンツが無秩序に流通し、ユーザ間で無断でコピーが行われるといった事態は好ましいことではない。

本発明は、このような状況に鑑みてなされたものであり、ユーザがコンテンツの正規な購入処理を行なって利用権に基づいた正当なコンテンツ利用を可能とするとともに、コンテンツを購入を伴わないコンテンツ試聴、あるいは試写を行なうことを可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

本発明は、さらに、試聴データ、試写データの無秩序な二次流通の防止を可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

本発明の第 1 の側面は、

暗号化されたコンテンツの復号及び利用を制御する情報処理装置であって、

- 5 コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報（usage right）に基づいて、該コンテンツの利用を制御する制御手段と、

製造時に記録されたあるいはサービス登録時に取得されたデフォルト利用権情報を記録する記録手段とを備え、

- 10 前記制御手段は、前記コンテンツに前記デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可する

ことを特徴とする情報処理装置にある。

15

さらに、本発明の情報処理装置の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記制御手段は、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果

20 に基づいて前記コンテンツの再生を許可することを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、サービスへの登録要求を送信する送信手段と、登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を

25 受信する受信手段とを備えることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記受信手段は、さらに前記コンテンツの復号に必要な鍵情報を受信することを特徴とする。

さらに、本発明の第2の側面は、

暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理装置であって、

5 登録要求を受信する受信手段と、

前記登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信する送信手段と、

を備えることを特徴とする情報処理装置にある。

10 さらに、本発明の情報処理装置の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする。

15

さらに、本発明の第3の側面は、

暗号化されたコンテンツの復号及び利用を制御する情報処理方法であって、

20 コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報 (usage right) に基づくコンテンツ利用を制御する制御ステップを有し、

前記制御ステップは、

25 前記コンテンツに、製造時に記録されたデフォルト利用権情報、あるいはサービス登録時に取得されたデフォルト利用権情報に対応することを示す情報が含まれているか否かを検証するステップと、

デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可するステップと、

を含むことを特徴とする情報処理方法にある。

さらに、本発明の情報処理方法の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記制御ステップは、さらに、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可するステップを含むことを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、サービスへの登録要求を送信する送信ステップと、登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信ステップと、を含むことを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記コンテンツの復号に必要な鍵情報を受信するステップを含むことを特徴とする。

さらに、本発明の第4の側面は、
暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理方法であって、
登録要求を受信する受信ステップと、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信する送信ステップと、
を有することを特徴とする情報処理方法にある。

さらに、本発明の情報処理方法の一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に

再生を許可することが記述されていることを特徴とする。

さらに、本発明の第5の側面は、

5 暗号化されたコンテンツの復号及び利用を制御する情報処理を実行するコンピュータ・プログラムであって、
コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報 (u s a g e r i g h t) に基づくコンテンツ利用を制御する制御ステップを有し、

前記制御ステップは、

10 前記コンテンツに、製造時に記録されたデフォルト利用権情報、あるいはサービス登録時に取得されたデフォルト利用権情報に対応することを示す情報が含まれているか否かを検証するステップと、

デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツ
15 を復号し、利用することを許可するステップと、

を含むことを特徴とするコンピュータ・プログラムにある。

さらに、本発明のコンピュータ・プログラムの一実施態様において、前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記制御ステップは、さら
20 に、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可するステップを含むことを特徴とする。

25 さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、サービスへの登録要求を送信する送信ステップと、登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信ステップと、を含むことを特徴とする。

さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、前記コンテンツの復号に必要なとなる鍵情報を受信するステップを含むことを特徴とする。

5 さらに、本発明の第6の側面は、

暗号化されたコンテンツの利用条件（usage rules）が記述された利用権を発行する情報処理を実行するコンピュータ・プログラムであって、

登録要求を受信する受信ステップと、

10 前記登録要求に応じて、暗号化されたコンテンツの復号に必要なとなる鍵情報と、デフォルト利用権情報を送信する送信ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

さらに、本発明のコンピュータ・プログラムの一実施態様において、
15 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする。

20 さらに、本発明の第7の側面は、

暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置と、暗号化されたコンテンツの利用条件（usage rules）が記述された利用権を発行する利用権発行装置を有するコンテンツ利用管理システムであって、

25 前記コンテンツ利用装置は、

サービスへの登録要求を送信する送信手段と、

登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信手段とを備え、

前記利用権発行装置は、

前記登録要求を受信する受信手段と、

前記登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信する送信手段とを備えた構成、であることを特徴とするコンテンツ利用管理システムにある。

5

さらに、本発明の第8の側面は、

暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置と、暗号化されたコンテンツの利用条件 (u s a g e r u l e s) が記述された利用権を発行する利用権発行装置を有するコンテンツ利用管理システムにおけるコンテンツ利用管理方法であって、

10

前記コンテンツ利用装置から前記利用権発行装置に対してサービスへの登録要求を送信する登録要求送信ステップと、

前記利用権発行装置において、前記登録要求を受信し、該登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信するデータ送信ステップと、

15

前記コンテンツ利用装置において、デフォルト利用権情報を受信する受信ステップと、

を有することを特徴とするコンテンツ利用管理方法にある。

20

本発明の構成によれば、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報 (D e f a u l t U s a g e R i g h t) を取得し、コンテンツの購入処理を伴わない試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生が許可され、ユーザは、コンテンツの購入を実行することなく、コンテンツの試聴再生が可能となる。また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

25

さらに、本発明の構成によれば、コンテンツの購入処理を伴わない試聴処理においても、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB [EKB (H)] と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB [EKB (S)] に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴処理においても再生権限を限定した範囲として設定可能となる。

- 10 なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムを
- 15 コンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

- 20 なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

- 25 図1は、本発明を適用したコンテンツ提供システムの概要を示す図である。

図2は、クライアント、および各サーバ、管理システムの構成例を示す図である。

図3は、各種キー、データの暗号化処理、配布処理について説明する

ツリー構成図である。

図 4 は、各種キー、データの配布に使用される有効化キーブロック (EKB) の例を示す図である。

5 図 5 は、コンテンツキーの有効化キーブロック (EKB) を使用した配布例と復号処理例を示す図である。

図 6 は、有効化キーブロック (EKB) のフォーマット例を示す図である。

図 7 は、有効化キーブロック (EKB) のタグの構成を説明する図である。

10 図 8 は、ツリー構成におけるカテゴリ分割を説明する図である。

図 9 は、ツリー構成におけるカテゴリ分割を説明する図である。

図 10 は、ツリー構成におけるカテゴリ分割の具体例を説明する図である。

15 図 11 は、コンテンツ購入、または試聴処理における各エンティティ間の実行処理シーケンス (その 1) を示す図である。

図 12 は、管理システムにおいて実行するトランザクション ID 生成、発行処理手順を示すフロー図である。

図 13 は、コンテンツ購入、または試聴処理における各エンティティ間の実行処理シーケンス (その 2) を示す図である。

20 図 14 は、管理システムにおいて実行するダウンロード許可処理手順を示すフロー図である。

図 15 は、起動ファイルのデータ構成例を示す図である。

図 16 は、クライアントにおいて実行する起動ファイルに基づくアプリケーション実行手順を示すフロー図である。

25 図 17 は、サービスデータ、利用権情報のデータ構成例を示す図である。

図 18 は、コンテンツ購入処理における各エンティティ間の実行処理シーケンスを示す図である。

図 19 は、コンテンツ再生処理の概要を説明する図である。

図 20 は、有効化キーブロック (EKB) を適用したコンテンツ復号、利用処理例を説明する図である。

図 21 は、コンテンツ試聴処理における各エンティティ間の実行処理シーケンスを示す図である。

5 図 22 は、試聴コンテンツ再生処理の概要を説明する図である。

図 23 は、ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティティ間の処理シーケンス (その 1) を示す図である。

10 図 24 は、リストア処理要求ファイル [restore.dat] の構成例を示す図である。

図 25 は、MAC 生成処理構成を示す図である。

図 26 は、ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティティ間の処理シーケンス (その 2) を示す図である。

15 図 27 は、ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティティ間の処理シーケンス (その 3) を示す図である。

図 28 は、リコメンドファイルの生成処理フローを示す図である。

図 29 は、リコメンドファイル生成画面を示す図である。

20 図 30 は、リコメンドファイル構成例を示す図である。

図 31 は、リコメンドファイル中に格納されるコンテンツファイルの構成例を示す図である。

図 32 は、リコメンドファイル中に格納されるコンテンツ説明ファイルの表示例を示す図である。

25 図 33 は、リコメンドファイルを受領したクライアントにおけるライセンス情報取得処理フロー (その 1) を示す図である。

図 34 は、リコメンドファイルを受領したクライアントにおけるライセンス情報取得処理フロー (その 2) を示す図である。

発明を実施するための最良の形態

以下、本発明の構成について詳細に説明する。なお、説明は、以下に示す各項目に従って行なう。

- 5 1. コンテンツ提供システム概要
- 2. キー配信構成としてのツリー（木）構造について
- 3. EKBを使用したキーの配布
- 4. EKBのフォーマット
- 5. ツリーのカテゴリ分類
- 10 6. コンテンツ購入および試聴処理
- 7. バックアップ／リストア処理
- 8. リコメンドファイルによるコンテンツの二次配信

〔1. コンテンツ提供システム概要〕

- 15 図1は、本発明を適用したコンテンツ提供システムの概要を説明する図である。コンテンツの利用を行なうクライアント10は、コンテンツを利用、すなわち再生可能な機器としての情報処理装置である。例えばPC、PDA等、各種の情報処理装置が含まれる。クライアント10は、ソフトウェアとしてブラウザ11、クライアントアプリケーション12
- 20 を有し、CPU等の制御手段によりブラウザ11、クライアントアプリケーション12他のプログラムが実行される。

- 25 クライアントアプリケーション12は、クライアントにおけるコンテンツの購入および試聴処理、後段において説明するサービスデータ、コンテンツ利用権情報を含むライセンス情報の取得処理、コンテンツおよびライセンス情報のバックアップ／リストア処理、コンテンツ利用権の確認処理、コンテンツ再生管理処理、あるいは、二次配信用のコンテンツファイルとしてのリコメンドファイルの生成処理等を実行するアプリケーションであり、以下、詳細に説明する処理プログラムとして、ク

クライアントの情報処理装置に格納される。なお、本明細書においては、「試聴」は、音声データの試聴のみならず、画像データの試写を包含する意味として用いる。

- 5 クライアント10は、例えばインターネット等の通信網を介してショップサーバ21、ライセンスサーバ22、およびコンテンツサーバ23と接続される。コンテンツサーバ23は、クライアント10に対してコンテンツを提供する。ライセンスサーバ22は、クライアントが利用するコンテンツの利用権情報をクライアント10に対して提供する。また、
- 10 ショップサーバ21は、クライアント10がコンテンツを購入する際の窓口として機能し、購入または試聴可能コンテンツをブラウザを介して提示し、クライアントからの購入あるいは試聴の要求を受け付ける。また、必要に応じて購入コンテンツに関する課金処理を行なう。
- 15 さらに、ショップサーバ21、およびライセンスサーバ22には、管理システム31が接続される。管理システム31は、ショップサーバ21が受け付けたクライアント10からのコンテンツ要求に対する許可情報として機能するトランザクションID (TID) の発行処理、コンテンツダウンロード許可情報の発行処理を行なう。また、管理システム
- 20 31は、ライセンスサーバ22に対して、コンテンツの利用権情報としての利用権データUsage Right) の発行許可を行なう。これらの処理の詳細は、後段で説明する。

- 25 なお、クライアント10は、ライセンスサーバ22からの利用権の取得、コンテンツサーバ23からのコンテンツ取得を、クライアントアプリケーション12の制御の下に実行し、ショップサーバ21の提供する情報の閲覧および決済処理は、クライアントアプリケーション12の制御の下にブラウザ11を起動して実行する。

図1には、クライアントおよび各サーバを1つずつ示してあるが、これらは例えばインターネット等の通信網上に多数接続され、クライアントは、様々なショップサーバに接続し、各ショップサーバで提供するコンテンツを自由に選択し、選択したコンテンツを格納したコンテンツサーバからコンテンツを取得し、取得したコンテンツの利用権を発行する
5 ライセンスサーバを選択して、その選択されたライセンスサーバから利用権を取得する。

コンテンツは、暗号化コンテンツとしてコンテンツサーバ23からクライアント10に提供される。さらに、ライセンスサーバ22からクライアント10に対しては、コンテンツに対応するコンテンツ利用権情報が提供され、クライアント10のクライアントアプリケーション12が、
10 利用権情報を検証し、利用権があると判定された場合に暗号化コンテンツを復号して利用する。

クライアント10は、コンテンツ利用権に基づくコンテンツ利用を可能とするための鍵情報として、有効化キーブロック (EKB: Enabling Key Block)、デバイス・ノード・キー (DNK: Device Node Key) 等の鍵データを保持する。有効化キーブロック (EKB: Enabling Key
20 Block)、デバイス・ノード・キー (DNK: Device Node Key) は、コンテンツの利用を正当なコンテンツ利用権を有するユーザデバイスにおいてのみ暗号化コンテンツを復号して利用可能とするためのコンテンツ利用に必要な暗号鍵を取得するための鍵データである。EKB, DNKについては、後段で説明する。

コンテンツサーバ23は、コンテンツを暗号化して、暗号化コンテンツをクライアント10に提供する。さらに、ライセンスサーバ22は、コンテンツ利用条件に基づいて利用権情報 (Usage Right) を生成してユーザデバイス30に提供する。さらに、管理システム31
25

の提供するデバイスノードキー（DNK：Device Node Key）、有効化キーブロック（EKB：Enabling Key Block）に基づいてサービスデータを生成してクライアント10に提供する。サービスデータは、暗号化コンテンツの復号処理の際に必要となるサービス・デバイスノードキー（SDNK）を持つ有効化キーブロック（EKB）を含む。

なお、コンテンツの利用条件には、利用期間の限定条件、コピーの回数制限、さらにコンテンツを同時に利用することができるポータブルメディア（PM：Portable Media）の数（いわゆるチェックアウト（Check-out）数に対応）の制限等がある。ポータブルメディア（PM：Portable Media）は例えばフラッシュメモリ、または小型HD、光ディスク、光磁気ディスク、MD（Mini Disk）等、ポータブルデバイスにおいて利用可能な記憶媒体である。

次に、図2を参照して、クライアント10、ショップサーバ21、ライセンスサーバ22、コンテンツサーバ23、管理システム31として機能可能な情報処理装置の構成例を示す。これらの各システムはCPUを持つ例えばPC、サーバ等のシステムにそれぞれの処理に応じた処理プログラムを格納することで実現される。

まず、図2を用いて各システムの構成例について説明する。CPU（Central Processing Unit）101は、ROM（Read Only Memory）102に記憶されている各種プログラム、あるいは、記憶部108に格納され、RAM（Random Access Memory）103にロードされたプログラムに従って各種処理を実行する。タイマ100は計時処理を行ない、クロック情報をCPU101に供給する。

ROM（Read Only Memory）102は、CPU101が使用するプログラムや演算用のパラメータ、固定データ等を格納する。RAM（Random Access Memory）103は、CPU101の実行において使用するプロ

グラムや、その実行において適宜変化するパラメータ等を格納する。これら各素子はCPUバスなどから構成されるバス111により相互に接続されている。

- 5 暗号化復号部104は、コンテンツの暗号化、復号処理、デバイスノードキー（DNK：Device Node Key）、有効化キーブロック（EKB：Enabling Key Block）の適用処理として、例えばDES（Data Encryption Standard）の暗号化アルゴリズムを適用した暗号処理、MAC生成、検証処理等を実行する。さらに、他の接続装置との間で実行されるコンテンツあるいはライセンス情報の送受信時の認証およびセッションキー共有処理等、各種暗号処理を実行する。
- 10

- コーデック部105は、例えばATRA C（Adaptive Transform Acoustic Coding）3方式、MPEG、JPEG方式等、各種方式のデータエンコード処理、デコード処理を実行する。処理対象データは、バス111、入出力インタフェース112、ドライブ110を介してリムーバブル記憶媒体121からまたは通信部109を介して入力する。また処理後のデータは、必要に応じて、リムーバブル記憶媒体121に格納し、または通信部109を介して出力する。
- 15

- 20 入出力インタフェース112には、キーボード、マウス等の入力部106、CRT、LCD等のディスプレイ、スピーカ等からなる出力部107、ハードディスク等の記憶部108、モデム、ターミナルアダプタ等によって構成される通信部109が接続され、例えばインターネット等の通信網を介したデータ送受信を行なう。
- 25

〔2. キー配信構成としてのツリー（木）構造について〕

次に、正当なコンテンツ利用権を有するクライアントにおいてのみコンテンツを利用可能とするための、ブロードキャストエンクリプション

(Broadcast Encryption) 方式の一態様であるツリー構成によるデバイスとキーの管理構成について説明する。

図 3 の最下段に示すナンバ 0 ~ 1 5 がコンテンツ利用を行なうクライアントとしてのユーザデバイスである。すなわち図 3 に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

各デバイス 0 ~ 1 5 は、製造時あるいは出荷時、あるいはその後において、図 3 に示す階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセット（デバイスノードキー（DNK：Device Node Key））をメモリに格納する。図 3 の最下段に示す K 0 0 0 0 ~ K 1 1 1 1 が各デバイス 0 ~ 1 5 にそれぞれ割り当てられたリーフキーであり、最上段の K R（ルートキー）から、最下段から 2 番目の節（ノード）に記載されたキー：K R ~ K 1 1 1 をノードキーとする。

図 3 に示すツリー構成において、例えばデバイス 0 はリーフキー K 0 0 0 0 と、ノードキー：K 0 0 0、K 0 0、K 0、K R を所有する。デバイス 5 は K 0 1 0 1、K 0 1 0、K 0 1、K 0、K R を所有する。デバイス 1 5 は、K 1 1 1 1、K 1 1 1、K 1 1、K 1、K R を所有する。なお、図 3 のツリーにはデバイスが 0 ~ 1 5 の 1 6 個のみ記載され、ツリー構造も 4 段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

25

また、図 3 のツリー構成に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成された DVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共

共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

- 5 これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0, 1, 2, 3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス
10 共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、図3の点線で囲んだ部分、すなわちデバイス0,
15 1, 2, 3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図3のツリー中に複数存在する。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

20

- なお、ノードキー、リーフキーは、ある1つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。こ
25 れらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行する。

このツリー構造において、図3から明らかなように、1つのグループ

に含まれる3つのデバイス0, 1, 2, 3はデバイスノードキー (DNK : Device Node Key) として共通のキーK00、K0、KRを含むデバイスノードキー (DNK : Device Node Key) を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00は、デバイス0, 1, 2, 3に共通する保有キーとなる。また、新たなキーKnewをノードキーK00で暗号化した値Enc (K00, Knew) を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc (K00, Knew) を解いて新たなキーKnewを得ることが可能となる。なお、Enc (Ka, Kb) はKbをKaによって暗号化したデータであることを示す。

また、ある時点tにおいて、デバイス3の所有する鍵 : K0011, K001, K00, K0, KRが攻撃者 (ハッカー) により解析されて露呈したことが発覚した場合、それ以降、システム (デバイス0, 1, 2, 3のグループ) で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー : K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代 (Generation) : tの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図4(A)に示す有効化キーブロック (EKB : Enabling Key Block) と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。なお、有効化キーブロック (EKB) は、図3に示すよ

うなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック (EKB) は、キー更新ブロック (KRB: Key Renewal Block) と呼ばれることもある。

5

図4 (A) に示す有効化キーブロック (EKB) には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図4の例は、図3に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図3から明らかなように、デバイス0, デバイス1は、更新ノードキーとして $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要であり、デバイス2は、更新ノードキーとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

図4 (A) のEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図4 (A) の下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図4 (A) の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4 (A) の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス $K0000$ 、 $K0001$ は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス $K0000$ 、 $K0001$ は、図4 (A) の上から3段目の暗号化キー

Enc (K 0 0 0, K (t) 0 0) を復号し K (t) 0 0、を取得し、
以下、図 4 (A) の上から 2 段目の暗号化キー Enc (K (t) 0 0,
K (t) 0) を復号し、更新ノードキー K (t) 0、図 4 (A) の上から
1 段目の暗号化キー Enc (K (t) 0, K (t) R) を復号し K (t)
5 Rを得る。このようにして、デバイス 0, 1, 2 は更新した鍵 K (t)
Rを得ることができる。なお、図 4 (A) のインデックスは、復号キー
として使用するノードキー、リーフキーの絶対番地を示す。

図 3 に示すツリー構造の上位段のノードキー : K (t) 0, K (t)
10 Rの更新が不要であり、ノードキー K 0 0 のみの更新処理が必要である
場合には、図 4 (B) の有効化キーブロック (E K B) を用いることで、
更新ノードキー K (t) 0 0 をデバイス 0, 1, 2 に配布することができる。

図 4 (B) に示す E K B は、例えば特定のグループにおいて共有する
新たなコンテンツキーを配布する場合に利用可能である。具体例として、
図 3 に点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体
を用いており、新たな共通のコンテンツキー K (t) c o n が必要であ
るとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー K 0
15 0 を更新した K (t) 0 0 を用いて新たな共通の更新コンテンツキー :
K (t) c o n を暗号化したデータ Enc (K (t), K (t) c o n)
20 を図 4 (B) に示す E K B とともに配布する。この配布により、デバイ
ス 4 など、その他のグループの機器においては復号されないデータとし
ての配布が可能となる。

25

すなわち、デバイス 0, 1, 2 は E K B を処理して得た K (t) 0 0
を用いて上記暗号文を復号すれば、t 時点でのキー、例えばコンテンツ
の暗号化復号化に適用するコンテンツキー K (t) c o n を得ることが
可能になる。

[3. E K Bを使用したキーの配布]

図 5 に、 t 時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツキー $K(t)_{con}$ を得る処理例として、 $K(t)_{00}$ を用いて新たな共通のコンテンツキー $K(t)_{con}$ を暗号化したデータ $Enc(K(t)_{00}, K(t)_{con})$ と図 4 (B) に示す E K B とを記録媒体を介して受領したデバイス 0 の処理例を示す。すなわち E K B による暗号化メッセージデータをコンテンツキー $K(t)_{con}$ とした例である。

図 5 に示すように、デバイス 0 は、記録媒体に格納されている世代： t 時点の E K B と自分があらかじめ格納しているノードキー K_{000} を用いて上述したと同様の E K B 処理により、ノードキー $K(t)_{00}$ を生成する。さらに、復号した更新ノードキー $K(t)_{00}$ を用いて更新コンテンツキー $K(t)_{con}$ を復号して、後にそれを使用するために自分だけが持つリーフキー K_{0000} で暗号化して格納する。

[4. E K B のフォーマット]

図 6 に有効化キープブロック (E K B) のフォーマット例を示す。バージョン 201 は、有効化キープブロック (E K B) のバージョンを示す識別子である。なお、バージョンは最新の E K B を識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キープブロック (E K B) の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ 203 は、有効化キープブロック (E K B) 中のデータ部の位置を示すポインタであり、タグポインタ 204 はタグ部の位置、署名ポインタ 205 は署名の位置を示すポインタである。

データ部 206 は、例えば更新するノードキーを暗号化したデータを格納する。例えば図 5 に示すような更新されたノードキーに関する各暗

号化キー等を格納する。

タグ部 207 は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図 7 を用いて説明する。図 7 では、データとして先に図 4 (A) で説明した有効化キーブロック (EKB) を送付する例を示している。この時のデータは、図 7 の表 (b) に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスは KR となる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図 7 の (a) に示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが 0、ない場合は 1 が設定される。タグは {左 (L) タグ, 右 (R) タグ} として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、L タグ = 0、右にはデータがないので、R タグ = 1 となる。以下、すべてのデータにタグが設定され、図 7 (c) に示すデータ列、およびタグ列が構成される。

タグは、データ $Enc(Kxxx, Kyyy)$ がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータ $Enc(Kxxx, Kyyy)...$ は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図 4 で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0 : $Enc(K(t)0, K(t)root)$

00 : $Enc(K(t)00, K(t)0)$

000 : $Enc(K((t)000, K(T)00)$

... のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

図 6 に戻って、E K B フォーマットについてさらに説明する。署名 (Signature) 2 0 8 は、有効化キーブロック (E K B) を発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。E K B を受領したデバイスは署名検証によって正当な有効化キーブロック (E K B) 発行者が発行した有効化キーブロック (E K B) であることを確認する。

15 [5. ツリーのカテゴリ分類]

ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

20 図 8 に階層ツリー構造のカテゴリの分類の一例を示す。図 8 において、階層ツリー構造の最上段には、ルートキー K r o o t 3 0 1 が設定され、以下の中間段にはノードキー 3 0 2 が設定され、最下段には、リーフキー 3 0 3 が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

25

ここで、一例として最上段から第 M 段目のあるノードをカテゴリノード 3 0 4 として設定する。すなわち第 M 段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第 M 段の 1 つのノードを頂点として以下、M + 1 段以下のノード、リーフは、そのカテゴリに含まれるデバ

イスに関するノードおよびリーフとする。

例えば図 8 の第 M 段目の 1 つのノード 305 にはカテゴリ [メモリスティック (商標)] が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード 305 以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

10 さらに、M 段から数段分下位の段をサブカテゴリノード 306 として設定することができる。例えば図に示すようにカテゴリ [メモリスティック] ノード 305 の 2 段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、[再生専用器] のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード 306 以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード 307 が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる [PHS] ノード 308 と [携帯電話] ノード 309 を設定することができる。

20 さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば 1 つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器 X Y Z 専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器 X Y Z にその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化

キーブロック (EKB) を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

5 このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック (EKB) を独自に生成して、
10 頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

15 本発明のシステムにおいては、図9に示されるように、ツリー構成のシステムで、キー管理が行われる。図9の例では、 $8 + 2^4 + 3^2$ 段のノードがツリー構造とされ、ルートノードから下位の8段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム (Tシステムと称する) が対応する。
20

すなわち、このTシステムのノードよりさらに下の階層の 2^4 段のノードに対応するキーが、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。この例の場合、これにより、
25 2^4 (約16メガ) のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の 3^2 段の階層により、 2^{3^2} (約4ギガ) のユーザ (あるいはユーザデバイス) を規定することができる。最下段の 3^2 段のノードからTシステムのノードまでのパス上の各ノードに対応するキーが、DNK (Device Node Key) を構成し、最下段のリー

フに対応するIDがリーフIDとされる。

例えば、コンテンツを暗号化したコンテンツキーは更新されたルートキーKR'によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、EKB内に配置される。EKBにおける末端から1つ上の段の更新ノードキーはEKBの末端のノードキーあるいはリーフキーによって暗号化され、EKB内に配置される。

- 10 ユーザデバイスは、サービスデータに記述されているDNKのいずれかのキーを用いて、コンテンツデータとともに配布されるEKB内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、EKB内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルートキーKR'を得ることができる。

- 20 上述したように、ツリーのカテゴリ分類により、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化キーブロック(EKB)を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

- 25 さらに、上述のツリー構成のデバイス管理によるEKB配信システムを適用して、複数のカテゴリに基づくEKB配信構成を採用したコンテンツ配信および利用形態について説明する。

図10を参照して2つのカテゴリについて説明する。図10に示すよ

うに、ルートノード 3 5 0 の下段に T システムノード 3 5 1 を設定し、その下段に T サービスノード 3 5 2、および T ハードノード 3 5 3 を設定する。T ハードノード 3 5 3 を頂点としたツリーは、ユーザデバイス機器自体をリーフ 3 5 5 として設定し、機器を対象として発行するハード対応 E K B [E K B (H)] を配信するカテゴリツリーである。一方、T サービスノード 3 5 2 を頂点としたツリーは、ユーザデバイス機器に提供するサービスに対応して発行するサービス対応 E K B [E K B (S)] を配信するカテゴリツリーである。

- 10 ハード対応 E K B [E K B (H)]、サービス対応 E K B [E K B (S)] とも、それぞれ正当な権限を持つデバイスに対して与えられる D N K (Device Node Key) すなわち、リーフから T システムのノードまでのパス上の各ノードに対応するキーを有することで、各 E K B の復号が可能となる。

15

[6 . コンテンツ購入および試聴処理]

次に、クライアントがコンテンツを購入または試聴する際の処理の詳細について、図 1 1 以下を参照して説明する。

- 20 図 1 1 は、クライアントアプリケーション、ブラウザを有する P C 等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるコンテンツ購入処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

- 25 まず、クライアント側において、コンテンツの購入を行なおうとするユーザは、自己の P C 等の通信可能な情報処理装置に U R L を指定 (ステップ (1)) し、ブラウザが介してショップサーバの提示するコンテンツリスト画面 (ショップページ) を読み出し (ステップ (2)) て、ディスプレイに表示 (ステップ (3)) する。

クライアントは、ショップサーバの提示するコンテンツリストからコンテンツを選択して、さらに、購入または試聴どちらかの指定（ステップ（４））を行なって、ブラウザを介してショップサーバに要求データ
5 を送信（ステップ（５））する。要求データには、コンテンツＩＤ（ＣＩＤ）、ショップサーバ識別子（ＳｈｏｐＩＤ）、および購入または試聴どちらかの指定データが含まれる。

ショップサーバは、クライアントからのコンテンツ購入、または試聴
10 要求を受信すると、管理システムに対して、コンテンツの提供の可否判定を要求（ステップ（６））する。この判定要求には、コンテンツＩＤ（ＣＩＤ）、ショップサーバ識別子（ＳｈｏｐＩＤ）が含まれる。

管理システムは、コンテンツの提供の可否判定要求を受信すると、ト
15 ランザクションＩＤ（ＴＩＤ）の発行処理（ステップ（７））を実行する。ランザクションＩＤ（ＴＩＤ）の発行処理の詳細を図１２のフローを参照して説明する。

管理システムは、まず、ステップＳ１０１において、乱数を発生し、
20 発生乱数に基づいて、ランザクションＩＤ（ＴＩＤ）を生成する。次に、ステップＳ１０２において、生成したランザクションＩＤ（ＴＩＤ）と、ショップサーバから指定されたコンテンツＩＤ（ＣＩＤ）とを対応付けてランザクションデータとして記憶部に格納する。次に、生成したランザクションＩＤ（ＴＩＤ）をショップサーバに対して出力、
25 発行する。

図１１のシーケンス図に戻る。管理システムは、ランザクションＩＤ（ＴＩＤ）の生成後、生成したランザクションＩＤ（ＴＩＤ）と価格情報をＴＩＤ情報としてショップサーバに送信（ステップ（８））す

る。ただし、価格情報は、コンテンツ購入時においてのみ要求される情報であり、コンテンツ試聴処理に際しては、含まれない。T I D情報を受信したショップサーバは、クライアントからの要求がコンテンツ購入である場合に、T I D情報に含まれる価格に基づいて、課金処理（ステップ（9））を実行する。

クライアントからの要求がコンテンツ購入ではなく、コンテンツ試聴要求である場合には、この課金処理（ステップ（9））は省略される。

次に、図 1 3 のシーケンス図を参照して継続する処理について説明する。ショップサーバは、コンテンツ購入処理においては、課金が行われたことを条件として、またコンテンツ試聴処理においては、管理システムからの T I D 情報の受信を条件として、購入または試聴要求対象のコンテンツのダウンロード許可要求を管理システムに対して送信（ステップ（10））する。

管理システムは、ダウンロード許可要求を受信すると、ダウンロード許可要求検証処理（ステップ（11））を実行する。ダウンロード許可要求検証処理の詳細を図 1 4 のフローを参照して説明する。

20

管理システムは、まず、ステップ S 2 0 1 において、受信したダウンロード許可要求に含まれるトランザクション I D（T I D）と、先に生成し、記憶部に格納したトランザクション I D（T I D）とを照合し、さらにステップ S 2 0 2 において、照合の成立したトランザクション I D（T I D）に対応して記録されたコンテンツ I D（C I D）を取得し、ステップ S 2 0 3 において、C I D に対応するコンテンツのダウンロード許可を発行する。

図 1 3 のシーケンス図に戻り、説明を続ける。管理システムは、ダウ

ダウンロード許可要求検証処理（ステップ（11））の後、コンテンツのダウンロード許可をショップサーバに対して発行（ステップ（12））する。ダウンロード許可には、トランザクションID（TID）、コンテンツサーバURL（C-URL）、ライセンスサーバURL（L-URL）、コンテンツID（CID）、利用権情報ID（UID）、商品（コンテンツ）URL（S-URL）、サービスIDが含まれる。

ショップサーバは、管理システムからダウンロード許可を受信すると、クライアントアプリケーションにおけるコンテンツの利用（再生処理等）プログラムを起動させるための起動ファイルを生成してクライアントのブラウザを介してクライアントアプリケーションに対して送付する。

起動ファイルの例を図15を参照して説明する。起動ファイル360は、先に管理システムが生成したトランザクションID（TID）、クライアントが購入あるいは試聴するコンテンツID（CID）、管理システムが生成したダウンロード許可情報に含まれる利用権情報ID（UID）、管理システムが生成したダウンロード許可情報に含まれるサービスID、ライセンスサーバURL、商品（コンテンツ）URL、さらに、処理が購入であるか試聴であるかの識別データが含まれる。

なお、処理が購入であるか試聴であるかの識別データとしては、起動ファイルに設定される拡張子を購入であるか試聴であるかによって区別して設定し、これをクライアントアプリケーションが判別して、それぞれのアプリケーションを起動するようにしてもよい。

クライアントアプリケーションは、起動ファイルに応じて、アプリケーションを起動（ステップ（15））する。

クライアントアプリケーションにおいて実行するアプリケーション起動処理について、図16を参照して説明する。ステップS301において、まず、起動ファイルに設定されたサービスID対応のサービスデータをクライアントシステムとしての情報処理装置に格納されている
5 か否かを判定する。

サービスデータは、クライアントが各種のサービス、例えばコンテンツ利用サービスを受領したい場合、ライセンスサーバから受領するもので、例えば特定のサービスプロバイダの提供サービスの一括したサービス
10 利用権を認めるデータである。図17(a)にサービスデータのデータ構成例を示す。

図17(a)に示すように、サービスデータ370には、EKB配信ツリーにおいて設定されるクライアントに固有のリーフID、サービス
15 識別子としてのサービスID、さらにデバイスノードキー(DNK)をルートキー(Kroot)で暗号化したデータ、E(Kroot, DNK)が含まれる。サービスデータを受領するためには、クライアントは、ライセンスサーバに対する登録処理が必要とされる。登録処理は、図13に示す処理ステップ(15)、(16)の処理に対応する。

20

図16に示すステップS301において、サービスID対応のサービスデータを保有していないと判定すると、ステップS302において登録処理を実行して、サービスデータを受領する。

25

さらに、この登録処理時に、デフォルト利用権情報がライセンスサーバからクライアントに対して発行される。利用権情報は、通常は、購入コンテンツの利用条件を格納し、コンテンツの購入に対応して発行されるものであるが、デフォルト利用権情報は、コンテンツの購入を条件として発行するものではなく、クライアントの登録処理、あるいはサービ

データの発行処理を条件として発行する。このデフォルト利用権情報は、後段で説明するコンテンツの試聴処理の際の有効なコンテンツ利用権情報として適用される。

- 5 図 1 7 (b) に利用権情報のデータ構成例を示す。図 1 7 (b) に示すように、利用権情報 3 7 1 には、利用権情報識別子としての利用権情報 I D、発行日時情報としてのタイムスタンプ、クライアントに固有のリーフ I D、コンテンツ対応である場合は、コンテンツ I D、さらに、利用条件対象コンテンツ種別情報が格納される。

- 10 デフォルト利用権情報の場合は、特定の購入コンテンツに対応して発行されるものではないため、コンテンツ I D は省略、あるいは試聴可能なコンテンツに共通な I D が設定される。また、利用条件対象コンテンツ種別情報として、例えば試聴フラグがオン (O N) として設定された
15 コンテンツについての利用が許可される設定とする。コンテンツ 3 7 2 には図 1 7 (c) に示すように、試聴フラグ 3 7 3 が設定され、試聴フラグ 3 7 3 がオン (O N) の設定コンテンツであれば、試聴が許可されたコンテンツであることを示し、試聴フラグがオフ (O F F) の設定コンテンツであれば、試聴が許可されていないコンテンツであることを示す。
20 。

- クライアントアプリケーションは、試聴コンテンツ再生時には、デフォルト利用権情報を参照して、再生許可の有無を判定するとともに、コンテンツのフラグの検証を実行して、コンテンツの再生を行なうことになる。この処理については、後段で説明する。
25 。

図 1 6 の処理フローに戻りアプリケーション起動処理の処理手順について説明する。ステップ S 3 0 2 において、登録処理、すなわちライセンスサーバからのサービスデータ、デフォルト利用権情報の取得が終

了すると、ステップS 3 0 3において、ショップサーバから受信した起動ファイルが、購入用アプリケーションの起動ファイルであるか、試聴用アプリケーションの起動ファイルであるかを判別する。購入用アプリケーションの起動ファイルである場合は、ステップS 3 0 4に進み購入用アプリケーションを実行し、試聴用アプリケーションの起動ファイルである場合は、ステップS 3 0 5に進み試聴用アプリケーションを実行する。

次に、購入用アプリケーションの実行シーケンスについて、図18のシーケンス図を参照して説明する。

購入処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（21））する。これは、先にクライアントが購入要求を行なったコンテンツであり、利用権情報（図17（b）参照）に記録されたコンテンツID（CID）に対応するコンテンツである。クライアントアプリケーションは、コンテンツID（CID）によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

コンテンツサーバは、コンテンツダウンロード要求を受信すると、CIDに対応するコンテンツ情報をクライアントに送信（ステップ（22））する。このコンテンツ情報は、暗号化コンテンツを含み、図17（c）に示すように、コンテンツキー：Kcで暗号化されたコンテンツデータ：Enc（Kc, Content）、コンテンツキー：Kcをルートキー：Krootで暗号化したデータ：Enc（Kroot, Kc）、さらに：ルートキー：Krootを取得するためのEKB、さらに試聴フラグデータ、サービスID等の情報が付加されたファイルである。

コンテンツ情報を受領したクライアントは、受信コンテンツに対応す

る利用権情報 (U s a g e R i g h t) の取得要求をライセンスサーバに対して送信 (ステップ (23)) する。この要求には、先にショップサーバから受領した起動ファイル (図15参照) 中に含まれる利用権情報ID (U I D)、クライアント識別データとしてのリーフID、および先にショップサーバから受領した起動ファイル (図15参照) 中に含まれるトランザクションID (T I D) が含まれる。

10 ライセンスサーバは、利用権情報 (U s a g e R i g h t) の取得要求を受信すると、管理システムに対して、注文照会処理 (ステップ (24)) を行なう。この要求には、利用権情報ID (U I D)、トランザクションID (T I D) が含まれる。注文照会を受信した管理サーバは、注文照会応答として、利用権情報ID (U I D) に対応する利用条件を設定した応答情報をライセンスサーバに送信 (ステップ (25)) する。

15 応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報 (U s a g e R i g h t) を生成して、クライアントに対して発行 (ステップ (26)) する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェックアウト処理等の各種処理の許可情報によって構成される。

20

利用権情報 (U s a g e R i g h t) を受信したクライアントは、先にコンテンツサーバから受信したコンテンツについて、利用権情報 (U s a g e R i g h t) に記録された利用条件に基づいてコンテンツの利用が可能となる。ユーザからコンテンツID (C I D)、利用権
25 情報 (U s a g e R i g h t) IDを指定したコンテンツ再生要求 (ステップ (27)) があると、クライアントアプリケーションは、利用条件に従ったコンテンツ再生を実行 (ステップ (28)) する。

基本的なコンテンツ再生処理の手順について、図19を参照して説明

する。前述の説明から理解されるように、コンテンツサーバ382からクライアント383に対してコンテンツが提供されるとともに、ライセンスサーバ381からクライアント383にライセンスとして、サービスデータ、利用権情報 (U s a g e R i g h t) が与えられる。

5

コンテンツは、コンテンツキー: K cにより、暗号化されており (E n c (K c, C o n t e n t)、コンテンツキーK cは、E K Bから取得可能なルートキーK r o o tから得られるキーである。

10

クライアント383は、ライセンスサーバから受領したサービスデータからデバイスノードキー (D N K) を取得し、取得したD N Kに基づいてコンテンツファイルのE K Bを復号して、ルートキー: K r o o t を取得し、さらに、取得したルートキー: K r o o tを用いて、E n c (K r o o t, K c) を復号してコンテンツキー: K cを取得し、取得したコンテンツキー: K cをにより暗号化コンテンツ: E n c (K c, C o n t e n t) の復号処理を実行してコンテンツを取得し、再生する。

15

サービスデータ、利用権情報 (U s a g e R i g h t) と対応付けたコンテンツ再生処理の詳細について、図20を参照して説明する。

20

図20は、ハード対応E K B [E K B (H)]、サービス対応E K B [E K B (S)] を適用したコンテンツの復号処理に基づくコンテンツ利用処理シーケンスを説明した図である。

25

図20に示すサービスデータ401、および利用権情報403は、ライセンスサーバから受領するデータであり、暗号化コンテンツファイル402はコンテンツサーバから受領するデータである。サービスデータ401は、リーフ識別子としてのリーフID、適用するE K Bのバージョン、さらに、サービス対応E K B [E K B (S)] の復号に必要なサ

ービス対応デバイスノードキー (SDNK) を、ハード対応カテゴリツリーに対応して設定されるルートキー K_{root} ' によって暗号化したデータ $E(K_{root}', SDNK)$ を格納している。

- 5 暗号化コンテンツファイル 402 は、サービス対応のカテゴリツリーに対応して設定されるルートキー K_{root} を格納したサービス対応 $EKB[EKB(S)]$ 、ルートキー K_{root} でコンテンツ ID (CID) と、コンテンツ暗号処理および復号処理に適用するコンテンツキー (K_c) とを暗号化したデータ $E(K_{root}, CID + K_c)$ 、および、
10 コンテンツ (Content) をコンテンツキー K_c で暗号化したデータ $E(K_c, Content)$ を含むファイルである。

- また、利用権情報 403 は、リーフ ID と、コンテンツの利用条件情報を格納したデータである。コンテンツの利用条件情報には、コンテンツ
15 ツに対応して設定される利用期間、利用回数、コピー制限等の様々な利用条件が含まれる。利用権情報 403 を受領したユーザデバイスは、利用権情報をコンテンツに対応するセキュリティ情報として格納するか、あるいは、コンテンツの索引データとしての AV インデックスファイル内に格納する。

- 20 例えば、PC 等の大容量の記憶手段を有し、プロセッサ等の処理能力が高いユーザデバイスにおいては、利用権情報をコンテンツに対応するセキュリティ情報として格納することが可能であり、すべての利用権情報を格納して、コンテンツ利用の際にすべての利用権情報を参照した処理を行なうことが好ましい。一方、大容量の記憶手段を持たず、またプロ
25 セッサ等の処理能力が低いポータブルデバイス (PD) 等のユーザデバイスにおいては、選択された情報からなる利用権情報 403 をコンテンツの索引データとしての AV インデックスファイル内に格納して、コンテンツ利用の際に AV インデックスファイル内の利用条件情報を参

照した処理を行なう等の処理が可能である。

ユーザデバイスは、図 20 に示すステップ S 5 0 1 において、ハード
対応のデバイスノードキー (HDNK) 4 1 2 を適用して、ハード対応
5 の EKB (H) 4 1 1 の復号処理を実行し、EKB (H) 4 1 1 から、
ハード対応カテゴリツリーに対応して設定されるルートキー K r o o
t' を取得する。DNK を適用した EKB の処理は、先に図 5 を参照し
て説明した手法に従った処理となる。

10 次に、ステップ S 5 0 2 において、EKB (H) から取り出したルー
トキー K r o o t' を用いて、サービスデータ 4 0 1 内の暗号化データ
E (K r o o t', SDNK) の復号処理を実行し、サービス対応 EKB
B [EKB (S)] の処理 (復号) に適用するデバイスノードキー (S
DNK) を取得する。

15

次に、ステップ S 5 0 3 において、サービスデータから取り出したデ
バイスノードキー (SDNK) を用いて、暗号化コンテンツファイル 4
0 2 内に格納されたサービス対応 EKB [EKB (S)] の処理 (復号)
を実行し、サービス対応 EKB [EKB (S)] 内に格納されたサービ
20 ス対応カテゴリツリーに対応して設定されるルートキー K r o o t を
取得する。

次に、ステップ S 5 0 4 において、サービス対応 EKB [EKB (S)]
から取り出したルートキー K r o o t を用いて、暗号化コンテンツファ
25 イル 4 0 2 内に格納された暗号化データ E (K r o o t, CID + Kc)
の復号処理を実行し、コンテンツ ID (CID) と、コンテンツキー (K
c) を取得する。

次に、ステップ S 5 0 5 において、暗号化コンテンツファイル 4 0 2

から取り出したコンテンツID (CID) と、利用権情報内に格納されたコンテンツIDのマッチング (照合) 処理を実行する。マッチング処理により、コンテンツの利用が可能であることが確認されると、ステップS506において、暗号化コンテンツファイル402から取り出した
5 コンテンツキー (Kc) を適用して、暗号化コンテンツファイル402に格納された暗号化コンテンツE (Kc, Content) を復号してコンテンツの再生を行なう。

上述したように、コンテンツ利用機器としてのハードウェアに対応して
10 て設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB [EKB (H)] と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB [EKB (S)] をそれぞれ個別にユーザに対して提供し、それぞれのEKBに対する正当なDNKを有するユーザのみがサービスの利用を行なう
15 ことが可能となる。

サービス対応EKB [EKB (S)] を復号するためのDNK、すなわちSDNKは、コンテンツに対応したサービスデータ401として提供可能であり、またSDNKを正当なハードウェア対応のDNK、すな
20 わちHDNKを有する機器のみが取得可能なハード対応カテゴリツリーに対応して設定されるルートキーKroot' を適用して暗号化した構成としたので、正当なHDNKを有するユーザデバイスのみが、SDNKを取得でき、サービスが利用となる。

25 また、コンテンツ利用において、暗号化コンテンツファイル402から取得されるコンテンツ識別子 (CID) と、利用権情報から取得されるCIDとのマッチング処理を実行する構成としたので、利用権情報403を取得してCID情報を格納していることがコンテンツ再生プロセスの必須要件とすることが可能となり、利用条件に従ったコンテンツ

利用が実現される。

次に、クライアントアプリケーションの処理が試聴処理の実行アプリケーションである場合の処理について、図 2 1 のシーケンス図を参照して説明する。

試聴処理の場合、コンテンツ購入処理と同様、コンテンツ情報ファイル（図 1 9 参照）を取得してクライアントシステムの記憶部に格納し、その後、購入コンテンツと同様の処理によって再生することも可能であるが、記憶部に格納することなく、ストリーミング再生処理を実行する例について、図 2 1 を参照して説明する。

ストリーミング試聴処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（3 1））する。これは、先にクライアントが試聴要求を行なったコンテンツである。クライアントアプリケーションは、コンテンツ ID（CID）によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

コンテンツサーバは、ストリーミング再生の場合には、コンテンツの部分データ（コンテンツパート）を次々にクライアントに対して送信（ステップ（3 2））する。コンテンツパートを受信したクライアントは、受信コンテンツに対する再生処理を実行（ステップ（3 3））し、後続のコンテンツパートの要求をコンテンツサーバに送信する。この処理を連続して実行することによりストリーミング再生が行なわれる。

試聴再生処理の手順について、図 2 2 のフローを参照して説明する。ステップ S 7 0 1 において、クライアントアプリケーションは、コンテンツサーバから受信した試聴コンテンツファイル中からサービス ID

を取得する。

次にステップ S 7 0 2 において、抽出したサービス ID に対応するデフォルト利用権情報 (Default Usage Right) (図 1 7 (b) 参照) の有無を判定する。デフォルト利用権情報は、クライアントの登録処理時に、サービスデータ (図 1 7 (a) 参照) とともに、ライセンスサーバから送信される利用権情報であり、購入コンテンツに対応して発行される利用権情報と異なり、試聴可能なコンテンツに対して利用される利用権情報である。

コンテンツ試聴においては、デフォルト利用権情報 (Default Usage Right) を保有することが試聴実行許可条件であり、デフォルト利用権情報を保有していない場合は、ステップ S 7 0 5 に進み、エラーとしてコンテンツ再生が実行されず処理を終了する。

デフォルト利用権情報 (Default Usage Right) が格納されている場合は、ステップ S 7 0 3 において、デフォルト利用権情報を検証し、利用権情報の記録を確認する。デフォルト利用権情報には、例えば試聴フラグオンのコンテンツの試聴許可、あるいは試聴可能なコンテンツ ID 情報が格納されており、これらの情報を取得する。

次にステップ S 7 0 4 において、デフォルト利用権情報 (Default Usage Right) の利用条件に基づいてコンテンツが再生される。なお、再生処理は、前述の図 1 9、図 2 0 を参照して説明したように、コンテンツサーバから受信する暗号化コンテンツの復号処理を伴う再生処理となる。

なお、コンテンツの購入処理を伴わない試聴処理においても、図 2 0 を参照して説明した購入コンテンツの再生と同様、EKB 処理に基づく

キー取得処理によってコンテンツ復号用のキーを取得することが必要となる。例えば、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB [EKB (H)] と、コンテンツ利用サービスに対応して設定された

5 カテゴリツリーに対応するEKBとしてのサービス対応EKB [EKB (S)] に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴においても再生権限を限定した範囲として設定可能となる。

10 上述したように、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報 (Default Usage Right) を取得し、コンテンツの購入処理を伴わない、試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生を可能とした構成であるので、ユーザは、コンテンツの購入を実行することなく、コンテンツ

15 の試聴再生が可能となり、また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

20 なお、図21のシーケンス図では、ストリーミング再生の例を示したが、試聴データをクライアントの記憶媒体に格納し、再生時に、デフォルト利用権情報 (Default Usage Right) の有無を判定して、デフォルト利用権情報の記録に基づいて再生を行なう構成とすることも可能である。

25

[7. バックアップ／リストア処理]

次にクライアントが購入したコンテンツまたはコンテンツ利用権情報についてのバックアップ処理、リストア処理について説明する。

リストア処理は、クライアントのコンテンツ購入時、あるいは購入後の処理として実行されるコンテンツ対応のライセンス情報、すなわちサービスデータ、利用権情報の再取得、格納処理、あるいはコンテンツの再取得処理として実行される。

5

処理態様としては、サービスデータ、利用権情報、コンテンツのいずれかの再取得、あるいはこれらの全データの再取得が可能である。以下に説明する実施例においては、サービスデータ、利用権情報、コンテンツ全データの再取得、格納処理シーケンス例を説明するが、必ずしもこれら全データを再取得する処理に限らず、いずれかのデータのみを選択的に再取得することも可能である。

10

図 2 3 以下を参照して、バックアップ／リストア処理の詳細について説明する。図 2 3 は、クライアントアプリケーション、ブラウザを有する P C 等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるバックアップ／リストア処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

15

クライアントは、前述したコンテンツ購入処理に従って、正規にコンテンツ購入を行なったものとする。図 2 3 に示すシーケンスは、コンテンツ購入に続いて実行されるシーケンスである。

20

コンテンツ購入処理を実行したクライアントは、バックアップ／リストアデータの取得のためのデータファイルとしてのリストア処理要求ファイル [r e s t o r e . d a t] を生成 (ステップ (5 0)) する。リストア処理要求ファイル [r e s t o r e . d a t] の構成を図 2 4 に示す。

25

図 2 4 に示すように、リストア処理要求ファイル [r e s t o r e . d a t] は、E K B 配信ツリーにおけるクライアント識別データとしてのリーフ I D と、ハッシュ (h a s h) 値、例えば M A C (Message Authentication Code) からなる検証データによって構成される。クライアントアプリケーションは、管理システムと共有する秘密の鍵を適用してリーフ I D に基づく検証用データとしてのハッシュ値あるいは M A C を算出し、リーフ I D と検証用データからなるリストア処理要求ファイル [r e s t o r e . d a t] を生成する。

- 10 メッセージ認証符号 (M A C : Message authentication Code) は、データの改竄検証用のデータとして生成されるものである。D E S 暗号処理構成を用いた M A C 値生成例を図 2 5 に示す。図 2 5 の構成に示すように対象となるメッセージを 8 バイト単位に分割し、(以下、分割されたメッセージを M 1、M 2、...、M N とする)、まず、初期値 (Initial Value (以下、I V とする)) と M 1 を排他的論理和する (その結果を I 1 とする)。次に、I 1 を D E S 暗号化部に入れ、鍵 (以下、K 1 とする) を用いて暗号化する (出力を E 1 とする)。続けて、E 1 および M 2 を排他的論理和し、その出力 I 2 を D E S 暗号化部へ入れ、鍵 K 1 を用いて暗号化する (出力 E 2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきた E N がメッセージ認証符号 (M A C (Message Authentication Code)) となる。
- 15
20

M A C 値は、その生成元データが変更されると、異なる値になり、検証対象のデータ (メッセージ) に基づいて生成した M A C と、記録されている M A C との比較を行い、一致していれば、検証対象のデータ (メッセージ) は変更、改竄がなされていないことが証明される。

25

図 2 3 のシーケンスに戻り説明を続ける。クライアントは、ブラウザを介して管理システムの提供するリストアページにアクセス (ステップ

(51)) し、管理システムは、リストアページをクライアントのブラウザに提示(ステップ(52))する。管理システムの提示するリストアページは、リストア処理要求ファイル[r e s t o r e . d a t]のアップロード処理を実行する機能を持つページである。

5

クライアントは、管理システムの提示するリストアページにおいて、クライアントアプリケーションの生成したリストア処理要求ファイル[r e s t o r e . d a t]をアップロードする。リストア処理要求ファイル[r e s t o r e . d a t]は、図24を参照して説明したように、EKB配信ツリーにおけるクライアント識別データとしてのリーフIDと、例えばMAC(Message Authentication Code)からなるハッシュ(h a s h)値によって構成される。

10

管理システムは、リストア処理要求ファイル[r e s t o r e . d a t]を受信すると、クライアントと共有する秘密鍵を用いて、リーフIDに対するハッシュ値を算出し、算出ハッシュ値と、受信ハッシュ値の照合処理を行ない、受信データの検証(ステップ(54))を行なう。算出ハッシュ値と、受信ハッシュ値が適合したことを条件として、バックアップ/リストア用の起動ファイルをクライアントに送信(ステップ(55))する。起動ファイルの構成は、先に図15を参照して説明したと同様のファイル構成を持つ。

15

20

起動ファイルは、ブラウザからクライアントアプリケーションに渡され(ステップ(56))、起動ファイルの記述、あるいは拡張子によって判別選択されるバックアップ/リストア実行プログラムを起動し、リストア処理を実行(ステップ(57))する。

25

バックアップ/リストア処理の処理対象としては、サービスデータ、コンテンツ、コンテンツ利用権情報がある。サービスデータは前述した

ようにライセンスサーバに対する登録処理によって取得可能であり、コンテンツはコンテンツサーバから取得可能である。また、利用権情報は、ライセンスサーバから取得される。バックアップ／リストア処理においても、これらの各データは、それぞれのサーバから取得することになる。

5

まず、図 26 を参照して、バックアップ／リストア用サービスデータの取得処理について説明する。基本的に、この処理は、先に説明したコンテンツ購入時のクライアント登録処理と同様の手続きに従ったものとなる。

10

まず、クライアントアプリケーションは、登録要求をライセンスサーバに送信（ステップ（61））する。この登録要求には、管理システムが生成した起動ファイル中に含まれるトランザクション ID（TID）が含まれる。

15

登録要求を受信したライセンスサーバは、トランザクション ID（TID）に基づいて、バックアップ／リストア用サービスデータの取得であることを識別し、管理システムに対してサービス事前データ、すなわちサービスデータのバックアップ／リストア用データの割当要求（ステップ（62））を行なう。管理システムは、同じトランザクション ID に基づいて処理を実行したクライアント端末があるか否かを管理データに基づいて検証し、ある場合には、これらに対応付けて記憶（ステップ（63））する。これは、バックアップ／リストア処理の処理回数の上限（例えば 3 回）を設定し、上限を超える処理要求の場合には、処理

25

管理データの更新処理を実行した管理システムは、サービス事前データ割当応答をライセンスサーバに送信（ステップ（64））する。これは、バックアップ／リストア用サービスデータの発行許可情報として送

信されるものである。

サービス事前データ割当応答を受信したライセンスサーバは、バックアップ／リストア用サービスデータのクライアントに対する発行処理
5 を実行（ステップ（65））する。サービスデータは、先に図17（a）を参照して説明したように、サービスデータ370には、EKB配信ツリーにおいて設定されるクライアントに固有のリーフID、サービス識別子としてのサービスID、さらにデバイスノードキー（DNK）をルートキー（K_{root}）で暗号化したデータ、E（K_{root}, DNK）
10 が含まれる。

さらに、この処理時に、デフォルト利用権情報（図17（b）参照）もライセンスサーバからクライアントに対して発行される。先に説明したように、利用権情報は、通常は、購入コンテンツの利用条件を格納し、
15 コンテンツの購入に対応して発行されるものであるが、デフォルト利用権情報は、コンテンツの購入を条件として発行するものではなく、クライアントの登録処理、あるいはサービスデータの発行処理を条件として発行する。このデフォルト利用権情報は、前述したようにコンテンツの試聴処理の際の有効な利用権情報として適用される。

20

ライセンスサーバからサービスデータ、デフォルト利用権情報を受領したクライアントは、これらのデータをバックアップ用として、記憶手段に格納（ステップ（66））する。

25 次に、図27を参照して、コンテンツのバックアップ／リストア処理について説明する。コンテンツのバックアップ／リストア処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（71））する。これは、先にクライアントが購入したコンテンツと同一である。クライアントアプ

リケーションは、コンテンツID (CID) によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

コンテンツサーバは、コンテンツダウンロード要求を受信すると、CID
5 IDに対応するコンテンツ情報をクライアントに送信 (ステップ (7
2)) する。このコンテンツ情報は、暗号化コンテンツを含む情報である。先に図17(c)を参照して説明したように、コンテンツキー: K_cで暗号化されたコンテンツデータ: Enc (K_c, Content)、コンテンツキー: K_cをルートキー: K_{root}で暗号化したデータ:
10 Enc (K_{root}, K_c)、さらに: ルートキー: K_{root}を取得するためのEKB、さらに試聴フラグデータ、サービスID等の情報が付加されたファイルである。

コンテンツ情報を受領したクライアントは、受信コンテンツに対応する
15 利用権情報 (Usage Right) の取得要求をライセンスサーバに対して送信 (ステップ (73)) する。この要求には、起動ファイル (図15参照) 中に含まれる利用権情報ID (UID)、クライアント識別データとしてのリーフID、トランザクションID (TID) が含まれる。

20

ライセンスサーバは、利用権情報 (Usage Right) の取得要求を受信すると、管理システムに対して、注文照会処理 (ステップ (7
4)) を行なう。この要求には、利用権情報ID (UID)、トランザクションID (TID) が含まれる。注文照会を受信した管理サーバは、
25 注文照会応答として、利用権情報ID (UID) に対応する利用条件を設定した応答情報をライセンスサーバに送信 (ステップ (75)) する。

応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報 (Usage Right) を生成して、クライアント

に対して再発行（ステップ（76））する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェックアウト処理等の各種処理の許可情報によって構成される。

- 5 利用権情報（U s a g e R i g h t）を受信したクライアントは、先に受信したコンテンツと利用権情報とを記憶手段にバックアップデータとして格納する。

- 10 なお、バックアップ／リストア処理において、ライセンスサーバが発行する利用権情報は、正規なコンテンツ購入処理に際して発行する利用権情報とは異なる利用条件を設定したものとしてもよい。例えば、正規なコンテンツ購入時に発行する利用権情報に含まれる利用条件より厳しい条件、例えば利用期間の制限、コピー禁止、あるいはチェックアウト禁止といった条件を設定してバックアップ／リストア処理用の利用
15 権情報を設定発行してもよい。

[8 . リコメンドファイルによるコンテンツの二次配信]

- 20 次に、正規にコンテンツを購入したクライアントが、購入コンテンツを他のクライアントに提供するいわゆるコンテンツ二次配信を実行し、コンテンツ利用権をライセンスサーバから新たに配布することで、二次配信コンテンツを受領したクライアントにおいても正当なコンテンツ利用権を有することを条件としてコンテンツ利用を可能とし、さらに、コンテンツサーバからのコンテンツ配信負荷の軽減を実現した構成について説明する。

25

前述したように、コンテンツを再生利用するクライアントは、コンテンツを利用するためには、コンテンツサーバから暗号化されたコンテンツを受け取るとともに、ライセンスサーバから、ライセンス情報、すなわちサービスデータと、コンテンツに対応する利用権情報を受領するこ

とが必要となる。

ライセンス情報、すなわちサービスデータおよび利用権情報は、データ容量の小さいデータであるため、インターネット等の通信網を介した送受信が頻繁に行われたとしてもトラフィックの上昇も少なく、多大な配信時間がかかるといった問題は発生しない。しかし、一方、コンテンツは、音楽データ、画像データ、プログラム等様々であり、そのデータ容量も大きなものとなる。このような大容量のコンテンツを特定のコンテンツサーバから多くのクライアントに送信する場合には、送信時間が長くなり、コンテンツサーバの負担、ネットワークトラフィックの上昇等、様々な問題を発生させる。また、通信中の通信エラーによるコンテンツ配信エラーのトラブルも発生しかねない。

以下では、すでに正規なコンテンツを購入したクライアントの保有するコンテンツを他のクライアントに提供、すなわち二次配信を実行し、二次配信によるコンテンツの提供を受けたクライアントが、そのコンテンツのライセンス情報をライセンスサーバから受領することで、コンテンツサーバのクライアントに対するコンテンツ送信の負荷を減少させたシステムについて説明する。

20

図28にコンテンツを正規に受領したクライアントが他のクライアントに提供するコンテンツファイルを生成する処理手順を説明したフローを示す。なお、他のクライアントに提供するコンテンツを含むデータファイルをリコメンドファイルと呼ぶ。リコメンドファイルには、暗号化されたコンテンツを含むコンテンツファイル、および必要に応じてそのコンテンツの説明ファイル(例えばHTMLファイル)が含まれる。

25

図28の処理フローについて説明する。図28の処理を実行するクライアントは、前述したコンテンツ購入処理を実行し、正規にコンテンツ

を購入したクライアント、あるいは、リコメンドファイルを他のクライアントから受領し、その後の手続きにおいて正規なライセンスを取得したクライアントである。図 28 の処理は、クライアントアプリケーション（図 1 のクライアントアプリケーション 12）の 1 つの実行プログラムとしてクライアントシステムとしての情報処理装置の制御手段（CPU 等）による制御の下に実行される。ステップ S 801 において、クライアントは、自己のクライアント装置のディスプレイにリコメンドファイル作成画面を表示する。

- 10 リコメンドファイル作成画面例を図 29 に示す。クライアントが正規購入し、再生可能なコンテンツリスト 651 が中央に表示され、リコメンドファイルを生成する場合は、このコンテンツリスト 651 からコンテンツを選択（ステップ S 802）し、右側のリスト 654 にタイトル等を表示させる。コンテンツリスト 651 とリスト 654 間の移動処理
15 は、移動スイッチ 652、653 の操作によって実行される。

- リコメンドファイル生成対象コンテンツが選択されると、ステップ S 803 において、リコメンドファイル作成ボタン 655 が押下される。リコメンドファイル作成ボタン 655 が押下されると、ステップ S 80
20 4 において、リコメンドファイル内にコンテンツファイルに併せて説明ファイル、例えば HTML によって記述された説明ファイルを生成格納するか否かを選択する。これはユーザが任意に選択可能である。

- リコメンドファイルには、図 30（a）に示すように、暗号化コンテンツを含むコンテンツファイル 721 とコンテンツ説明ファイル 72
25 2 とを組み合わせたリコメンドファイル 720 構成と、図 30（b）に示すように、暗号化コンテンツを含むコンテンツファイル 721 のみからなるリコメンドファイル 730 構成との 2 つの態様があり、クライアントはその態様を自由に選択可能となる。

ステップ S 8 0 4 において、コンテンツ説明用ファイルの作成をしないと選択した場合は、図 3 0 (b) に示すコンテンツファイル 7 2 1 のみからなるリコメンドファイル 7 3 0 が生成される。

5

コンテンツファイルの構成を図 3 1 に示す。コンテンツファイル (M Q T ファイル) 7 2 1 には、暗号化コンテンツと、コンテンツ付加情報としてのメタ情報、さらにコンテンツ購入可能なショップを示すショップサーバ URL、コンテンツ識別子としてのコンテンツ ID (C I D) が含まれる。

10

なお、コンテンツファイルに格納される暗号化コンテンツは、コンテンツキー K c により暗号化されたコンテンツであり、コンテンツキー K c は、有効化キーブロック (E K B) 配信ツリー構成を適用して提供される有効化キーブロック (E K B) の復号により取得可能なキーの適用によってのみ取得可能なキーである。

15

一方、ステップ S 8 0 4 において、コンテンツ説明用ファイル作成を選択した場合は、ステップ S 8 0 6 に進み、コンテンツ説明ファイル (H T M L ファイル) 生成用の説明データ (メタデータ) をコンテンツ管理テーブルから取得する。コンテンツに対応するコンテンツ説明データは、上述したように暗号化コンテンツとともに、コンテンツファイル内にも格納されているが、正規にコンテンツ利用権を取得したクライアントは、コンテンツフィルから取り出したコンテンツ対応のメタデータをコンテンツ管理データとして、別ファイルに格納管理しており、リコメンドファイルにおいて生成される説明ファイル用のメタデータは、このコンテンツ管理データから抽出される。

20

25

ステップ S 8 0 7 において、コンテンツ管理データから抽出したメタ

データを、クライアントアプリケーションに設定されたテンプレートHTMLファイルに貼り付ける処理を実行し、コンテンツ対応の説明用HTMLファイルを生成し、ステップS808において、コンテンツファイルと説明用HTMLファイルからなるリコメンドファイルを生成する。

コンテンツ説明用データとしてのHTMLファイルの表示構成例を図32に示す。図32に示す例は、コンテンツが音楽データの場合の例である。説明用ファイルは、図32に示すように、音楽コンテンツの楽曲タイトル、アーティスト、発売元等の情報リスト、さらに、各種の操作、処理に関する説明が記述されている。リコメンドファイルを他のクライアントから受理したクライアントは、まずこの説明ファイルをオープンすることになる。

リコメンドファイルに格納されたコンテンツは暗号化されたコンテンツであり、正規なライセンス情報、すなわちサービスデータとコンテンツ対応の利用権情報を取得していない場合には再生することはできない。従って、リコメンドファイルを受領したクライアントがリコメンドファイルに格納されたコンテンツを利用する場合には、ライセンス情報を取得する手続きを実行することになる。

このライセンス情報取得処理について、図33、図34の処理フローを参照して説明する。リコメンドファイルを受領したクライアントは、図32に示す説明用ファイル（HTMLファイル）をオープンし、試聴、購入コンテンツ配信サイトボタン731をクリック（ステップS811）する。このクリック処理により、クライアントアプリケーションが起動（ステップS812）し、同じリコメンドファイルに格納されたコンテンツファイル（MQTファイル）（図31参照）を読み出して、コンテンツファイルからコンテンツID（CID）とショップURLを抽

出（ステップS 8 1 3）する。

このように、コンテンツ説明用ファイルの試聴、購入コンテンツ配信
サイトボタン7 3 1は、コンテンツファイルからショップサーバURL
5 を抽出し、抽出URLをブラウザに出力する処理を実行するクライアン
トアプリケーションプログラムを起動するリンクデータとして構成さ
れている。従って、リコメンドファイルを受領したクライアントが容易
にショップに接続して購入手続きを実行することが可能となる。

10 ステップS 8 1 4において、コンテンツファイルから抽出したコンテ
ンツID（CID）に基づいて、コンテンツファイル名を設定する。こ
れはクライアントアプリケーションにおいて予め設定されたファイル
名設定処理として実行され、例えばコンテンツのタイトル、アーティス
ト名、あるいはその複合データ等が適用される。ステップS 8 1 5では、
15 ステップS 8 1 4 5で設定したファイル名のコンテンツファイルがクラ
イアントの記憶部に格納される。

次に、ステップS 8 1 6において、ステップS 8 1 3でコンテンツフ
ァイルから抽出したショップURLがブラウザに渡され、ブラウザは受
20 領URLに対応するショップページをショップサーバから読み出す。

図3 4の処理フローのステップS 8 3 1において、ショップ画面がク
ライアントのディスプレイに表示される。以下の処理は、基本的には、
前述したコンテンツの購入処理、試聴処理のいずれかの処理と同様であ
25 り、先に図1 1、図1 3、図1 8、図2 1に従って説明した処理に従う
ことになる。ただし、コンテンツ自体はすでにコンクライアントが、リ
コメンドファイルから取得済みであるので、コンテンツサーバからのコ
ンテンツ受領処理は、省略される。

一連の処理の概略は、図 3 4 の処理フローのステップ S 8 3 2 以下に示す処理となる。まず、クライアントがショップサーバの提示するショップ画面において購入を指定してショップサーバに購入要求を出力すると、ショップサーバから購入用起動ファイルが送信される。これは、
5 先に、図 1 5 を参照して説明した起動ファイルと同様の構成を持つ。

次に、ステップ S 8 3 3 において、起動ファイルからコンテンツ識別子としてのコンテンツ ID (C I D) を取得する。次に、ステップ S 8 3 3 4 において、コンテンツ ID (C I D) に基づいて、コンテンツファイル名を算出する。クライアント装置にコンテンツを格納する際のコンテンツファイル名は、先の図 3 3 のフローの説明で述べたようにコンテンツ ID (C I D) に基づいて設定されることがクライアントアプリケーションにおいて規定され、C I D とファイル名の対応付けがなされている。
10

ステップ S 8 3 5 において、コンテンツ ID (C I D) から算出したファイル名と同一のファイル名のファイルが自己のクライアント装置の記憶部に格納されているか否かを判定する。コンテンツが格納されていない場合は、ステップ S 8 3 7 に進み、コンテンツサーバに接続して、コンテンツダウンロードを行なうことになる。この処理は、先に説明した
15
20 コンテンツ購入時の処理と同様である。

しかし、リコメンドファイルを受領しているクライアントは、先の図 3 3 のフロー中のステップ S 8 1 4, S 8 1 5 において、所定のファイル名を設定したコンテンツファイルを記憶部に格納しており、コンテンツのダウンロード処理は省略され、ステップ S 8 3 6 のコンテンツ利用
25 権情報の取得処理を実行し処理を終了することが可能となる。

クライアントがコンテンツ再生を実行する際は、前述したように、コンテンツ利用権情報に格納されたコンテンツ識別子 (C I D) と再生対

象コンテンツのコンテンツ識別子（C I D）との照合を行ないC I Dの一致を条件としてコンテンツ再生を実行する。また、有効化キーブロック（E K B）配信ツリー構成を適用して提供される有効化キーブロック（E K B）の復号によりコンテンツキーK cを取得し、取得したコンテンツキーK cを適用して暗号化コンテンツの復号処理を実行することにより、コンテンツを再生利用することが可能となる。

このように、すでにコンテンツを保有しているクライアントが暗号化コンテンツを含むコンテンツファイルと、説明用ファイルからなるリコメンドファイルを他のクライアントに提供することで、他のクライアントがコンテンツ配信サーバへのアクセスなしにコンテンツを受領することが可能となる。他のクライアントは、利用権情報を取得することを条件としてコンテンツの利用が可能となる構成であるので、不正なコンテンツの利用は防止される。

15

なお、図34のフローにおいてはサービスデータの取得処理については省略してあるが、サービスデータを保有していないクライアントがリコメンドファイルを受領した場合には、ライセンスサーバに対するアクセスを実行して登録処理を行ない、サービスデータを取得することが必要となる。この登録処理手続きは、先に図13、図16を参照して説明した処理に対応する処理となる。

20

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

25

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ
5 内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

例えば、プログラムは記憶媒体としてのハードディスクやROM
10 (Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。
15 このようなりムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなりムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータ
20 に無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体にインストールすることができる。

25 なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

以上、説明したように、本発明の構成によれば、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報（Default Usage Right）を取得し、コンテンツの購入処理を伴わない試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生が許可され、ユーザは、コンテンツの購入を実行することなく、コンテンツの試聴再生が可能となる。また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

さらに、本発明の構成によれば、コンテンツの購入処理を伴わない試聴処理においても、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するEKBとしてのハード対応EKB [EKB (H)] と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するEKBとしてのサービス対応EKB [EKB (S)] に対する正当なDNKを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴処理においても再生権限を限定した範囲として設定可能となる。

請求の範囲

1. 暗号化されたコンテンツの復号及び利用を制御する情報処理装置であって、

コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報 (usage right) に基づいて、該コンテンツの利用を制御する制御手段と、

製造時に記録されたあるいはサービス登録時に取得されたデフォルト利用権情報を記録する記録手段とを備え、

前記制御手段は、前記コンテンツに前記デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可する

ことを特徴とする情報処理装置。

2. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、

前記制御手段は、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可する

ことを特徴とする請求項 1 に記載の情報処理装置。

3. 前記情報処理装置は、さらに、

サービスへの登録要求を送信する送信手段と、

登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信手段と、

を備えることを特徴とする請求項 1 に記載の情報処理装置。

4. 前記受信手段は、さらに前記コンテンツの復号に必要な鍵情報を受信することを特徴とする請求項3に記載の情報処理装置。

5. 暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理装置であって、
登録要求を受信する受信手段と、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信する送信手段と、
を備えることを特徴とする情報処理装置。

6. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、

前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする請求項5に記載の情報処理装置。

7. 暗号化されたコンテンツの復号及び利用を制御する情報処理方法であって、

コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報 (usage right) に基づくコンテンツ利用を制御する制御ステップを有し、

前記制御ステップは、

前記コンテンツに、製造時に記録されたデフォルト利用権情報、あるいはサービス登録時に取得されたデフォルト利用権情報に対応することを示す情報が含まれているか否かを検証するステップと、

デフォルト利用権情報に対応することを示す情報が含まれている場合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテンツを復号し、利用することを許可するステップと、

を含むことを特徴とする情報処理方法。

8. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、

- 5 前記制御ステップは、さらに、前記コンテンツに試用コンテンツであることを示すフラグが含まれているかを検証し、検証結果に基づいて前記コンテンツの再生を許可するステップを含むことを特徴とする請求項7に記載の情報処理方法。

- 10 9. 前記情報処理方法は、さらに、
サービスへの登録要求を送信する送信ステップと、
登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信ステップと、
を含むことを特徴とする請求項7に記載の情報処理方法。

- 15 10. 前記情報処理方法は、さらに、
前記コンテンツの復号に必要となる鍵情報を受信するステップを含むことを特徴とする請求項9に記載の情報処理方法。

- 20 11. 暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理方法であって、
登録要求を受信する受信ステップと、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信する送信ステップと、
25 を有することを特徴とする情報処理方法。

12. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、
前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであ

ることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする請求項 11 に記載の情報処理方法。

13. 暗号化されたコンテンツの復号及び利用を制御する情報処理
5 を実行するコンピュータ・プログラムであって、
コンテンツ利用の指示に応じて、該コンテンツに対応する利用権情報
(u s a g e r i g h t) に基づくコンテンツ利用を制御する制御ス
テップを有し、
前記制御ステップは、
10 前記コンテンツに、製造時に記録されたデフォルト利用権情報、ある
いはサービス登録時に取得されたデフォルト利用権情報に対応するこ
とを示す情報が含まれているか否かを検証するステップと、
デフォルト利用権情報に対応することを示す情報が含まれている場
合に、前記デフォルト利用権情報に記述内容に基づいて前記コンテン
15 を復号し、利用することを許可するステップと、
を含むことを特徴とするコンピュータ・プログラム。

14. 前記デフォルト利用権情報に基づいて利用が許可される前記
コンテンツは、試用の目的で提供されるものであり、
20 前記制御ステップは、さらに、前記コンテンツに試用コンテンツであ
ることを示すフラグが含まれているかを検証し、検証結果に基づいて前
記コンテンツの再生を許可するステップを含むことを特徴とする請求
項 13 に記載のコンピュータ・プログラム。

- 25 15. 前記コンピュータ・プログラムは、さらに、
サービスへの登録要求を送信する送信ステップと、
登録要求に応じてライセンスサーバから送信されるデフォルト利用
権情報を受信する受信ステップと、
を含むことを特徴とする請求項 13 に記載のコンピュータ・プログラ

ム。

16. 前記コンピュータ・プログラムは、さらに、
前記コンテンツの復号に必要となる鍵情報を受信するステップを含むことを特徴とする請求項15に記載のコンピュータ・プログラム。

17. 暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する情報処理を実行するコンピュータ・プログラムであって、
10 登録要求を受信する受信ステップと、
前記登録要求に応じて、暗号化されたコンテンツの復号に必要となる鍵情報と、デフォルト利用権情報を送信する送信ステップと、
を有することを特徴とするコンピュータ・プログラム。

- 15 18. 前記デフォルト利用権情報に基づいて利用が許可される前記コンテンツは、試用の目的で提供されるものであり、
前記デフォルト利用権情報は、前記コンテンツに試用コンテンツであることを示すフラグが含まれている場合に再生を許可することが記述されていることを特徴とする請求項17に記載のコンピュータ・プログラム。
20 ラム。

19. 暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置と、暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する利用権発行装置を有するコンテンツ
25 利用管理システムであって、
前記コンテンツ利用装置は、
サービスへの登録要求を送信する送信手段と、
登録要求に応じてライセンスサーバから送信されるデフォルト利用権情報を受信する受信手段とを備え、

前記利用権発行装置は、

前記登録要求を受信する受信手段と、

前記登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信する送信手段とを備えた構成、

5 であることを特徴とするコンテンツ利用管理システム。

2.0. 暗号化されたコンテンツの復号及び利用を行うコンテンツ利用装置と、暗号化されたコンテンツの利用条件 (usage rules) が記述された利用権を発行する利用権発行装置を有するコンテンツ

10 利用管理システムにおけるコンテンツ利用管理方法であって、

前記コンテンツ利用装置から前記利用権発行装置に対してサービスへの登録要求を送信する登録要求送信ステップと、

前記利用権発行装置において、前記登録要求を受信し、該登録要求に応じて、暗号化されたコンテンツの復号に必要な鍵情報と、デフォルト利用権情報を送信するデータ送信ステップと、

15 前記コンテンツ利用装置において、デフォルト利用権情報を受信する受信ステップと、

を有することを特徴とするコンテンツ利用管理方法。

1/34

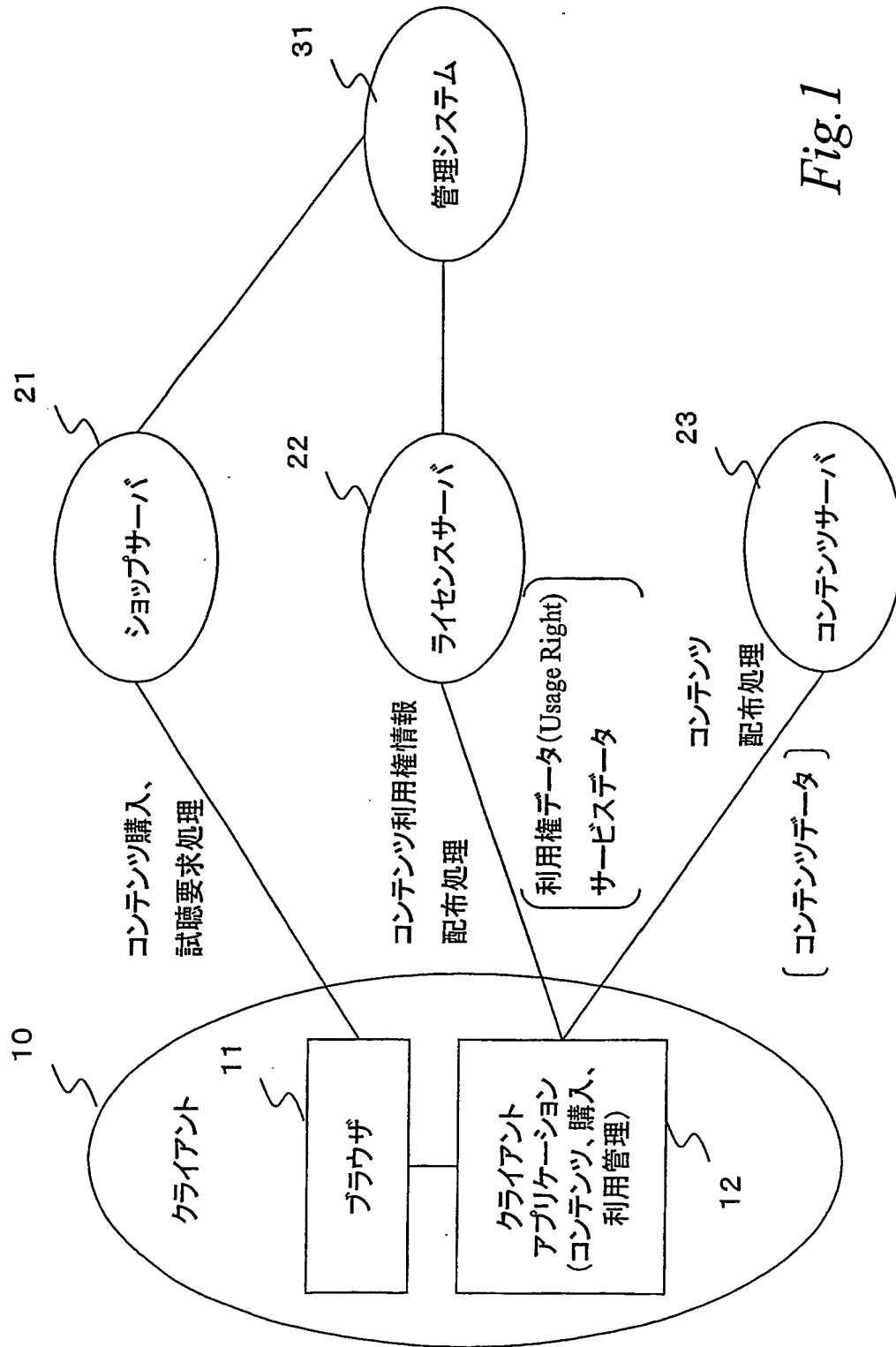


Fig. 1

2/34

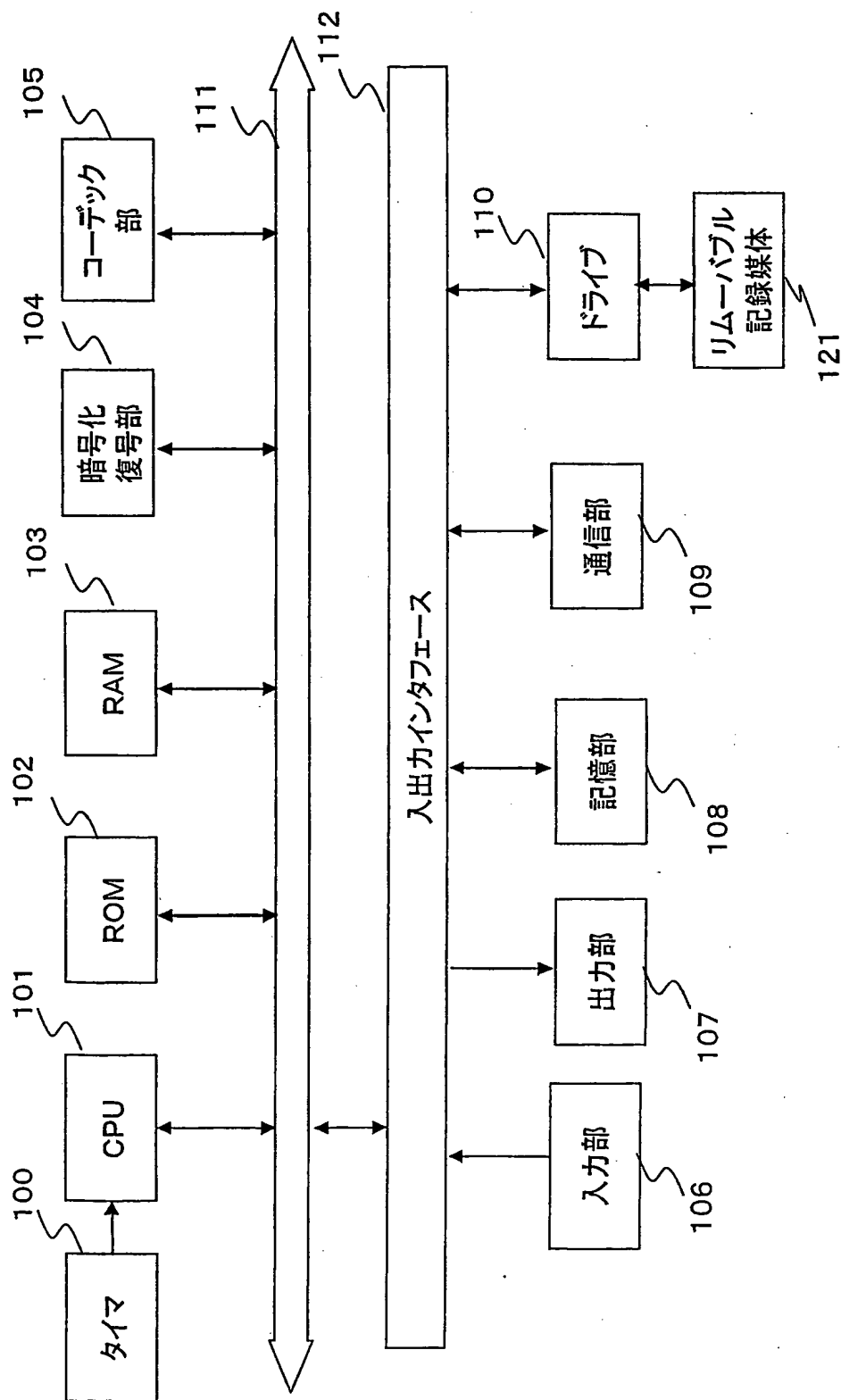
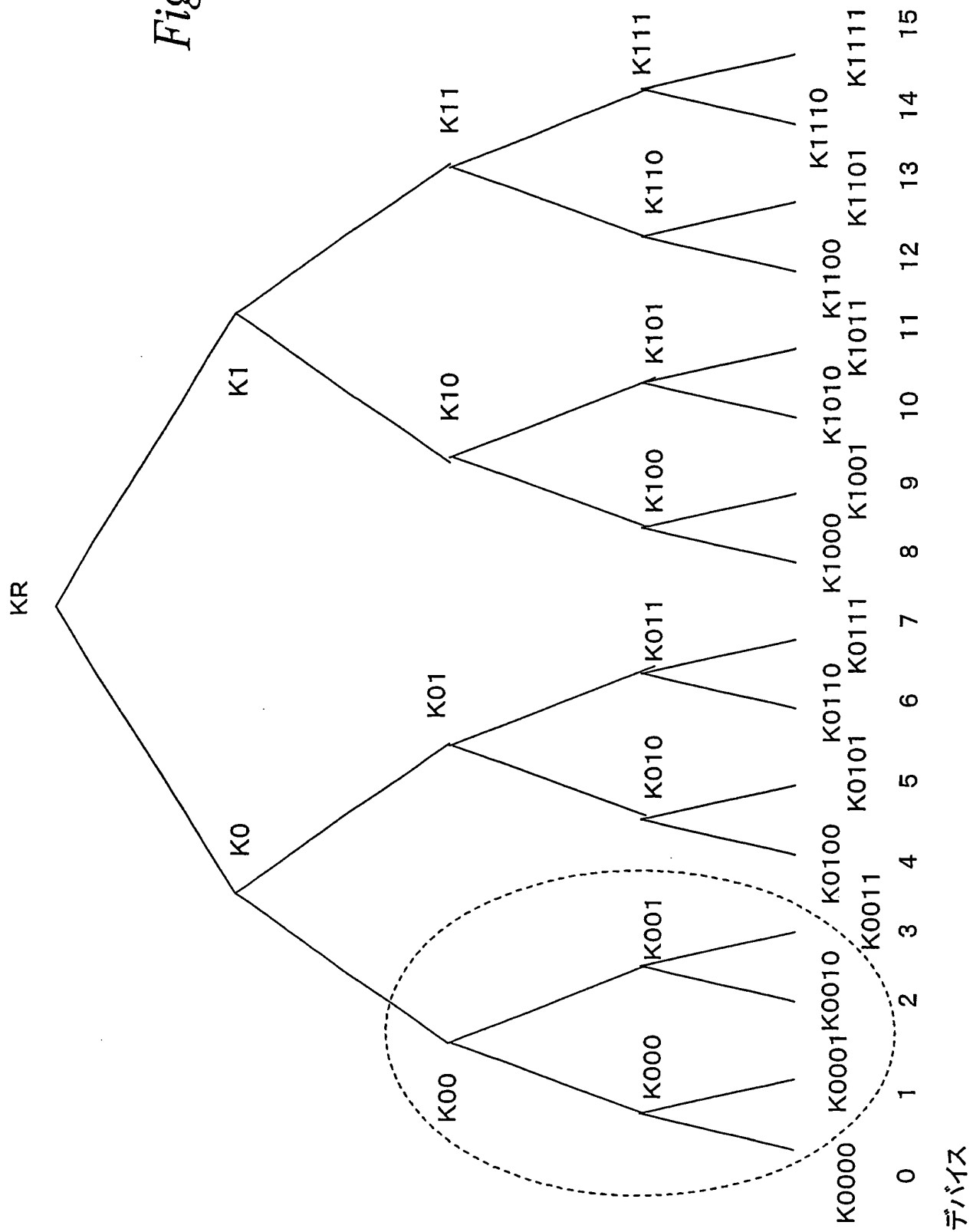


Fig. 2

3/34

Fig. 3



(A) 有効化キーブロック
(EKB:Enabling Key Block)例1

(B) 有効化キーブロック
(EKB:Enabling Key Block) 例2

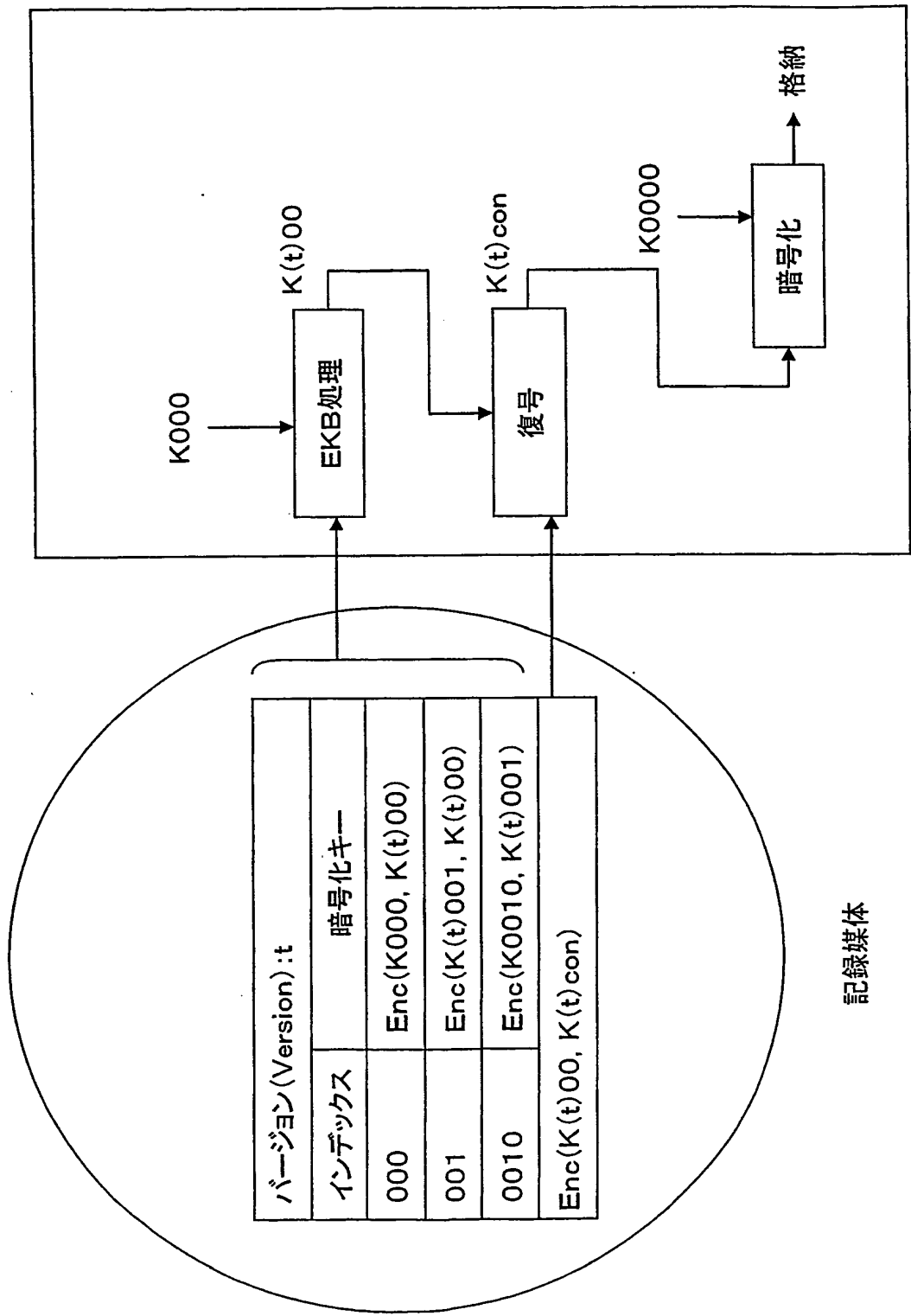
デバイス0, 1, 2にバージョン:tのノードキーを送付

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

Fig.4



デバイス0

Fig.5

6/34

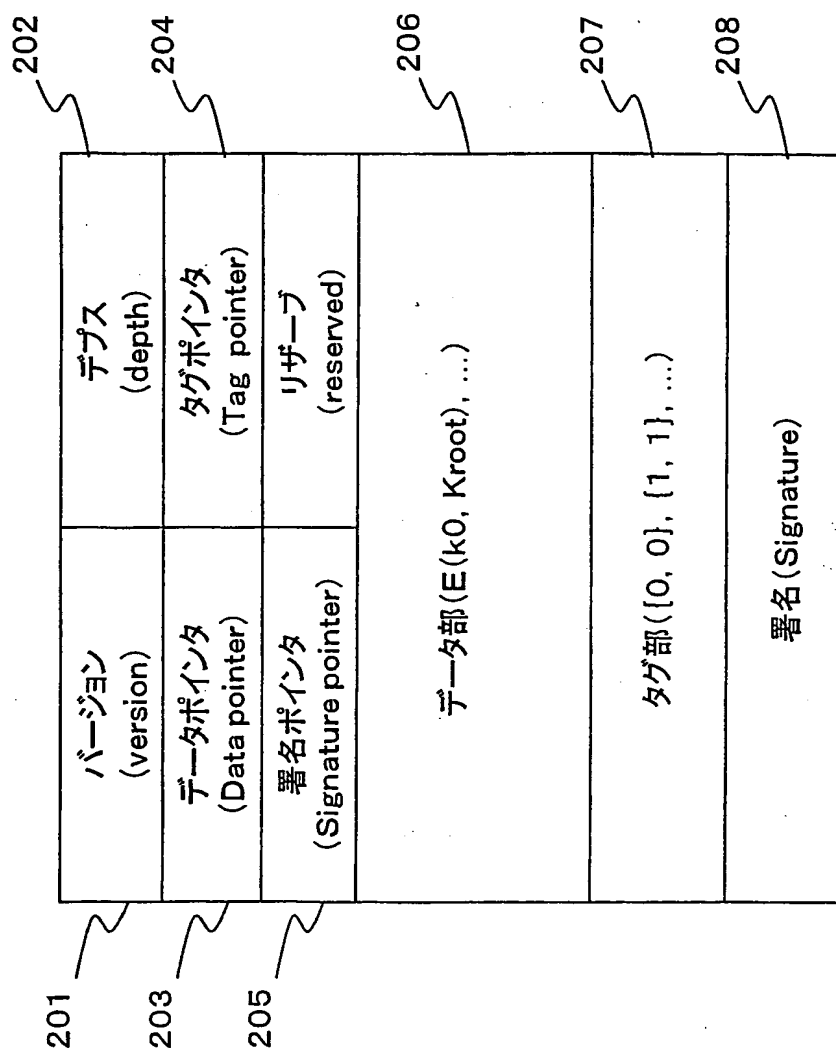


Fig. 6

8/34

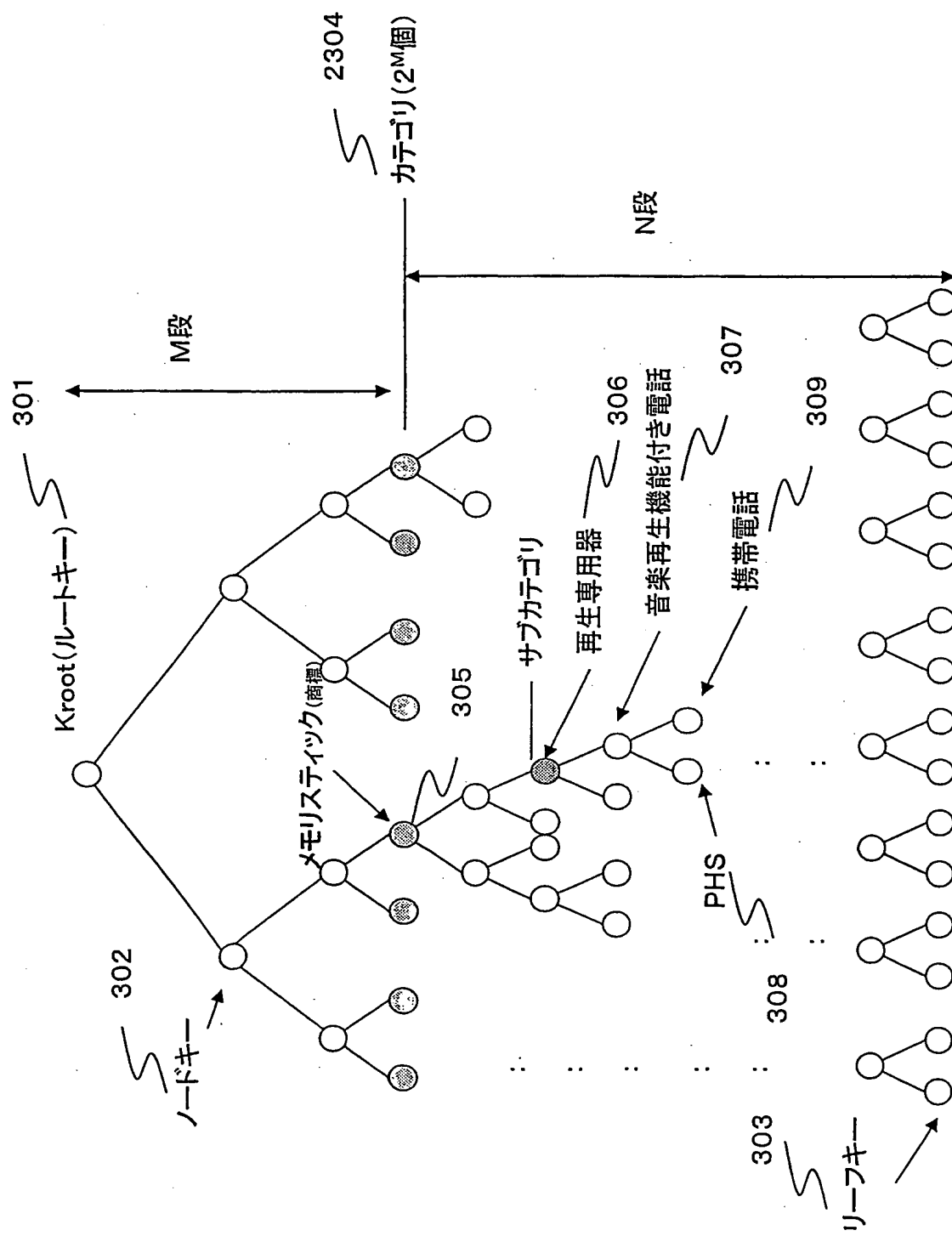


Fig.8

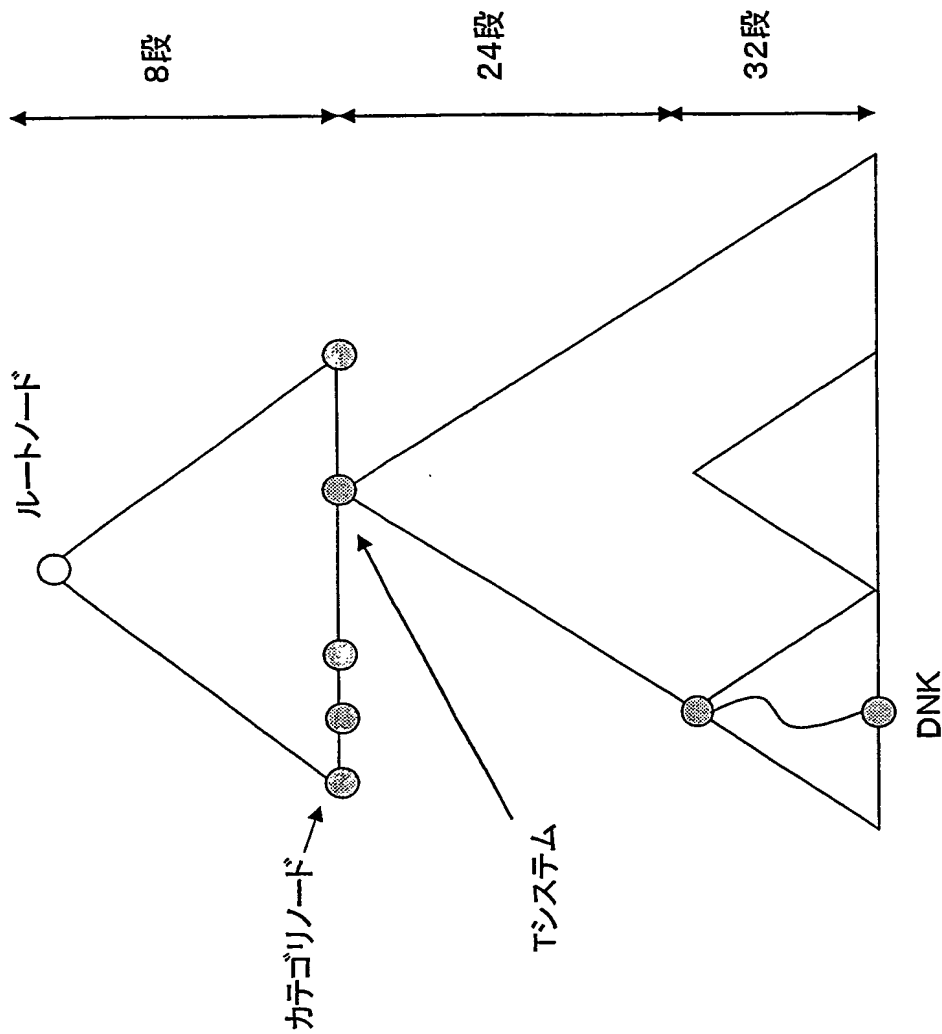
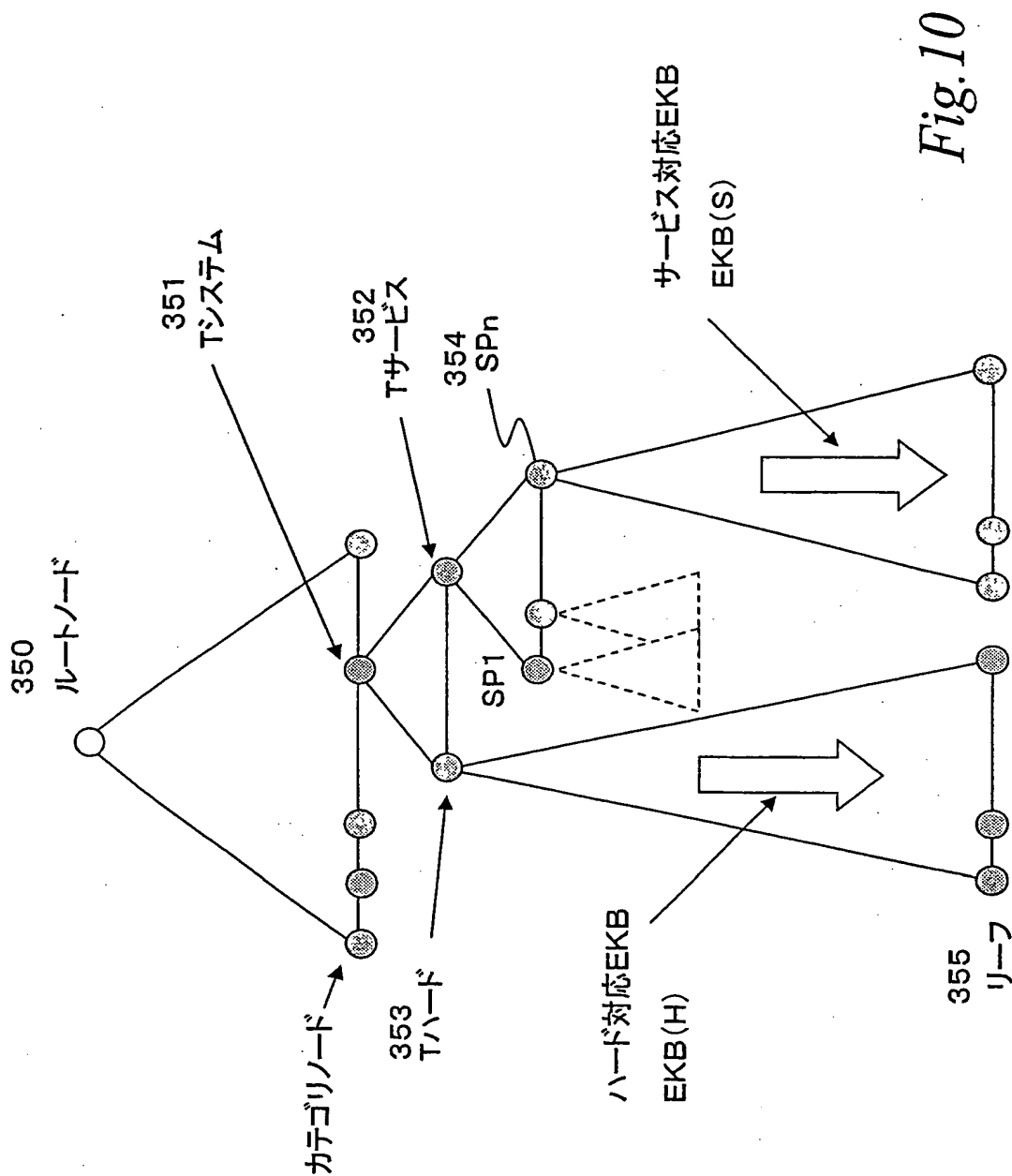


Fig. 9

10/34



11/34

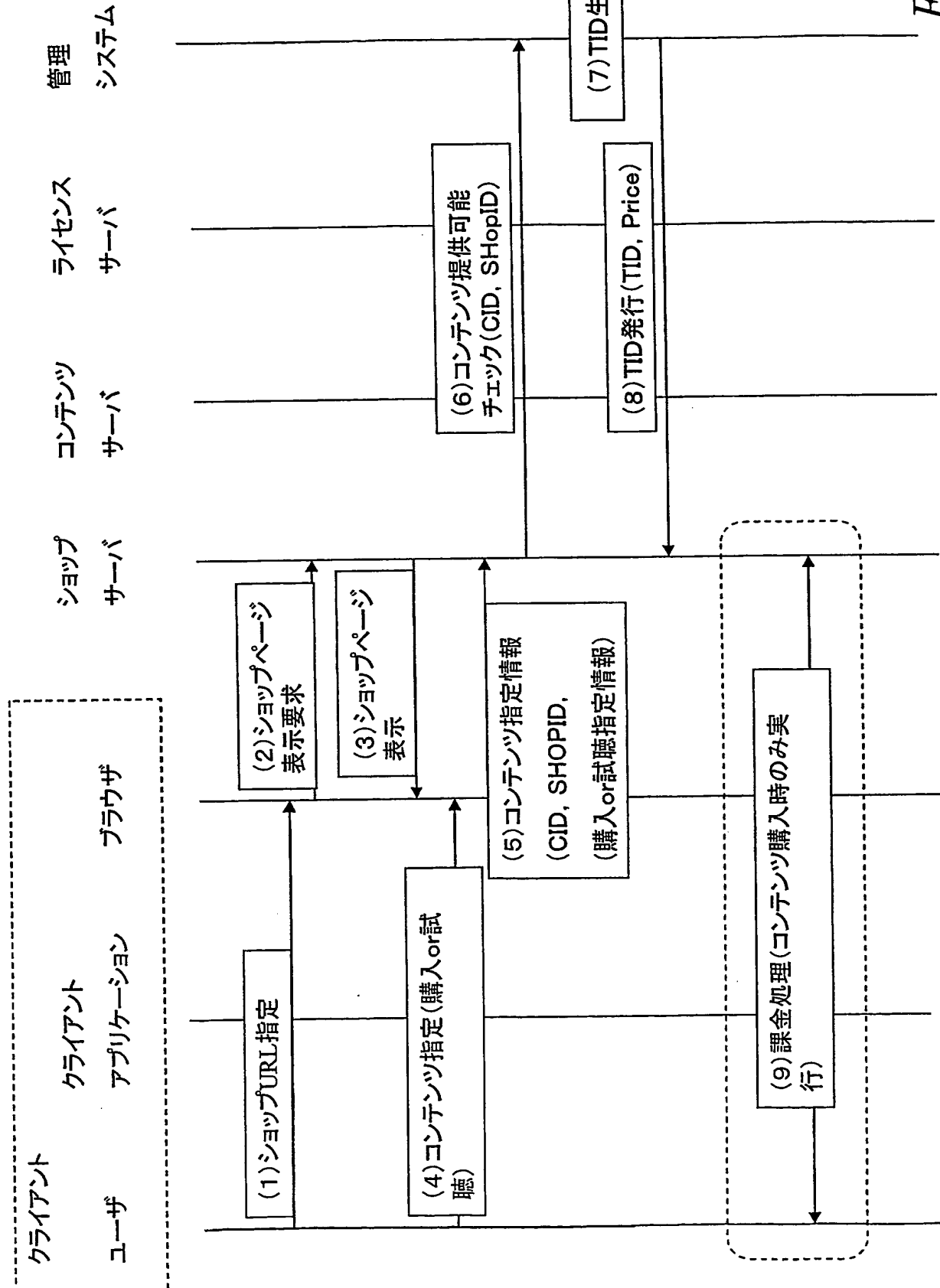


Fig. 11

12/34

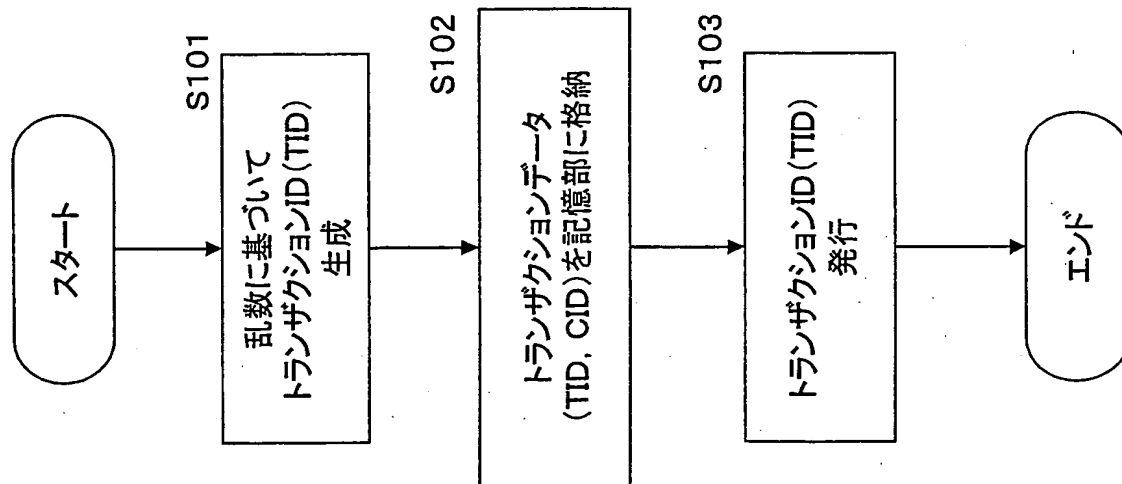


Fig.12

13/34

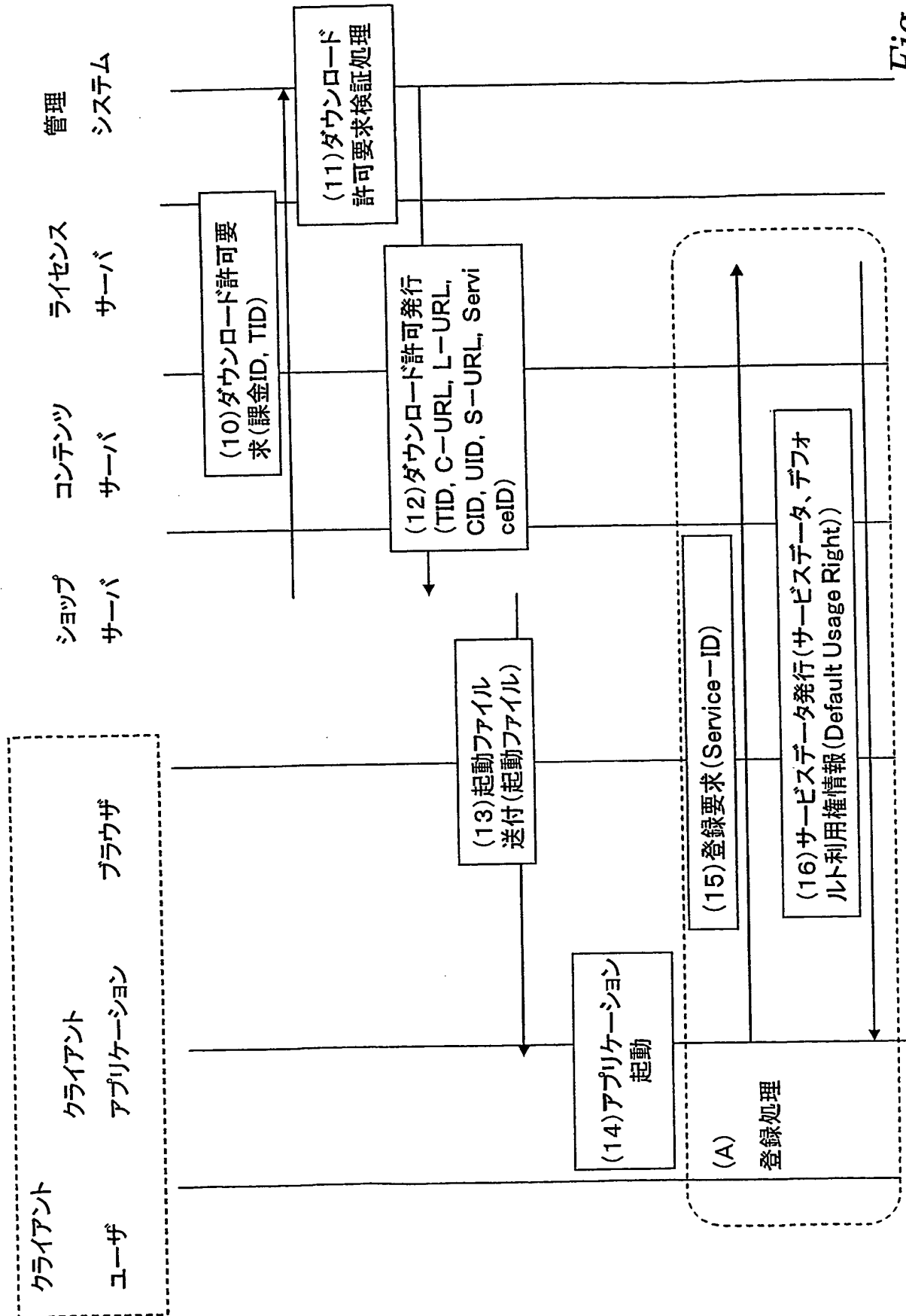


Fig. 13

14/34

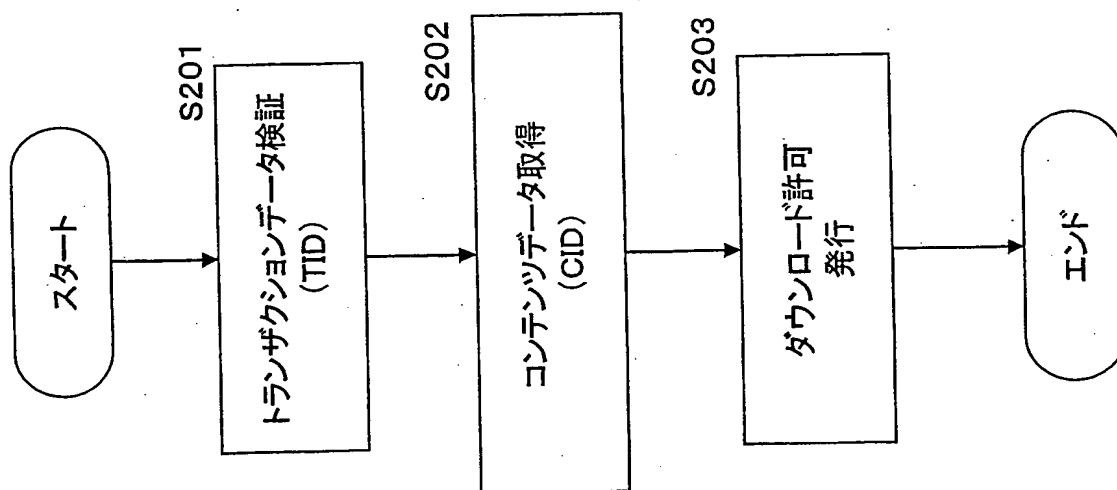


Fig. 14

16/34

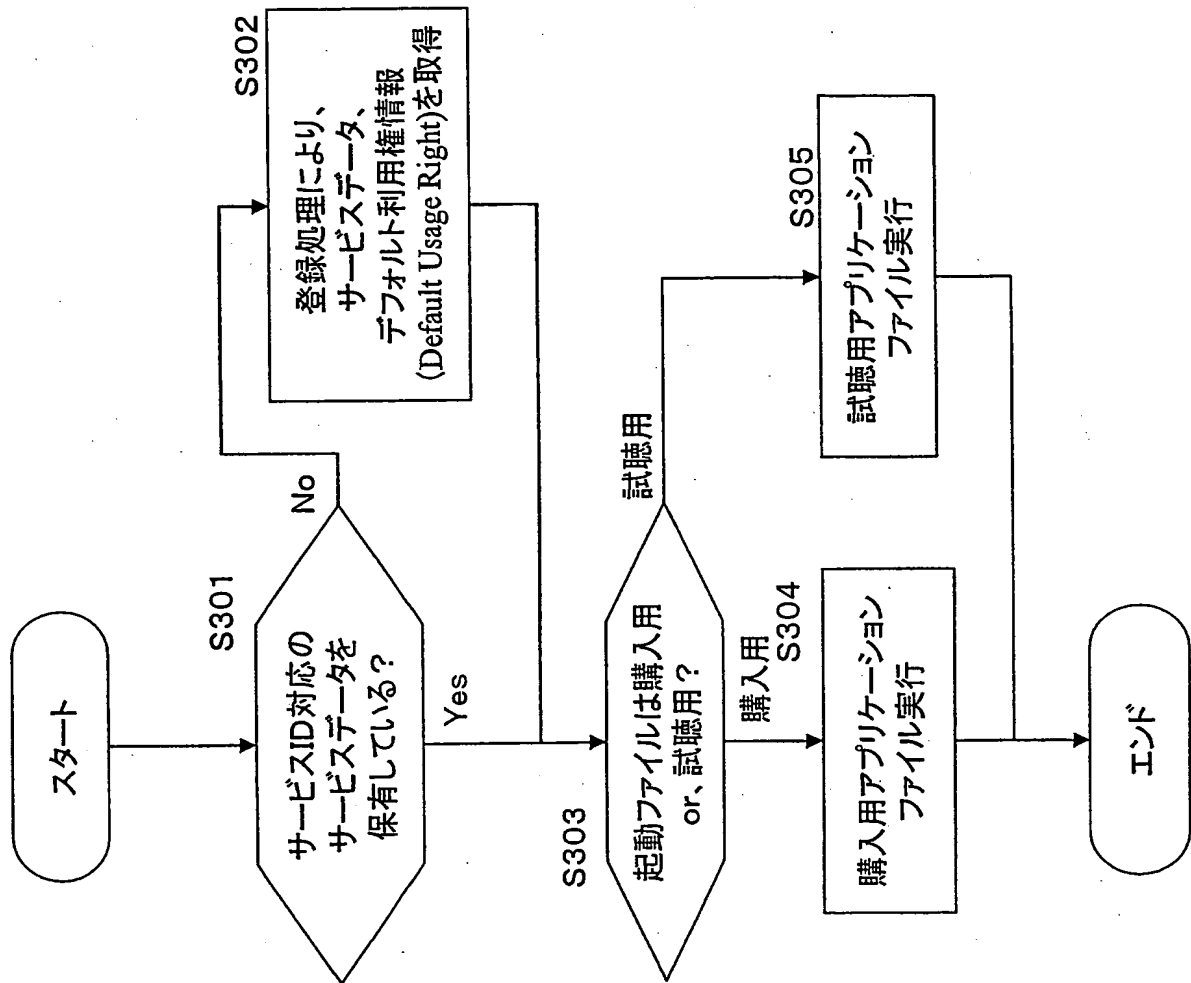


Fig. 16

17/34

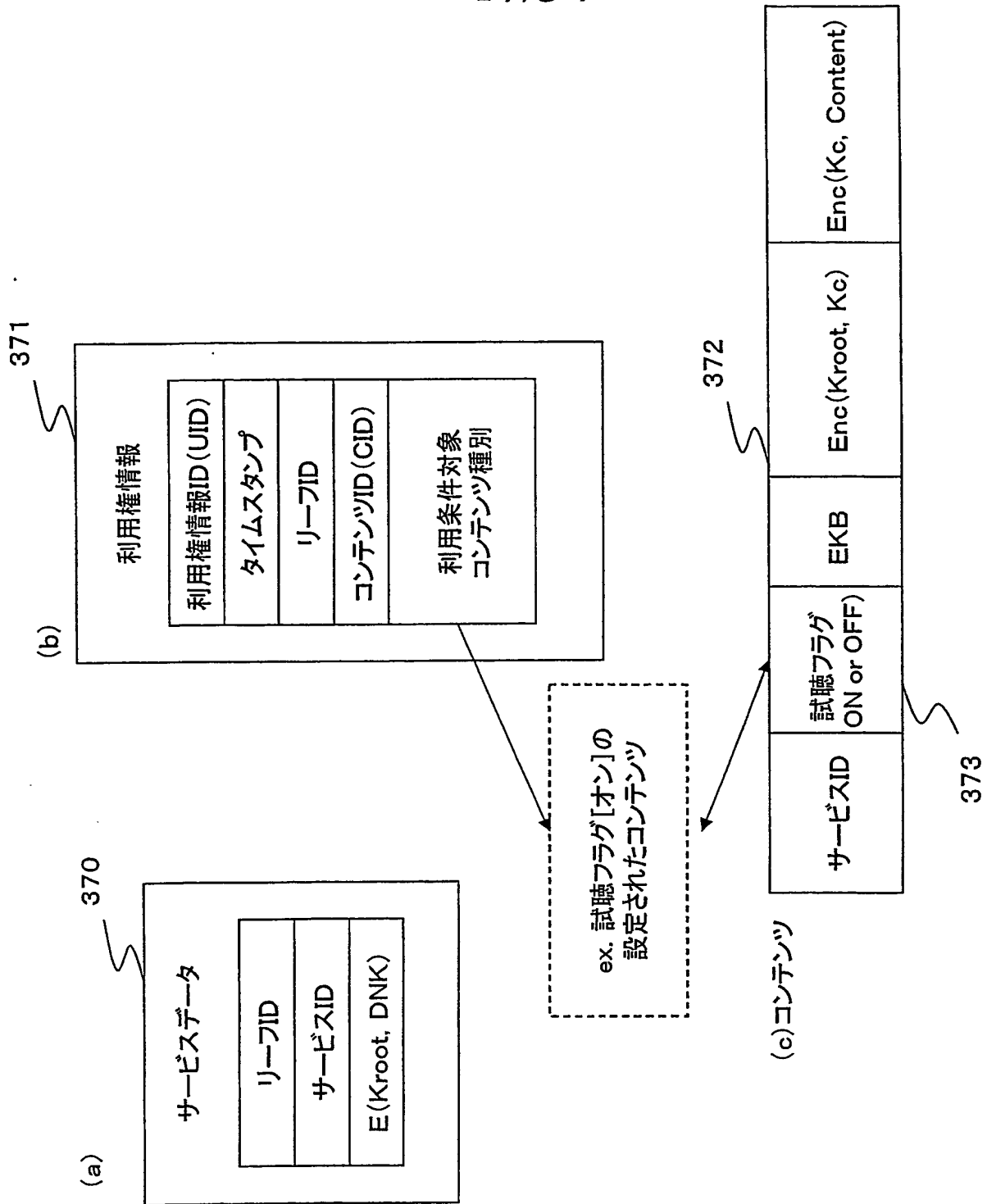


Fig. 17

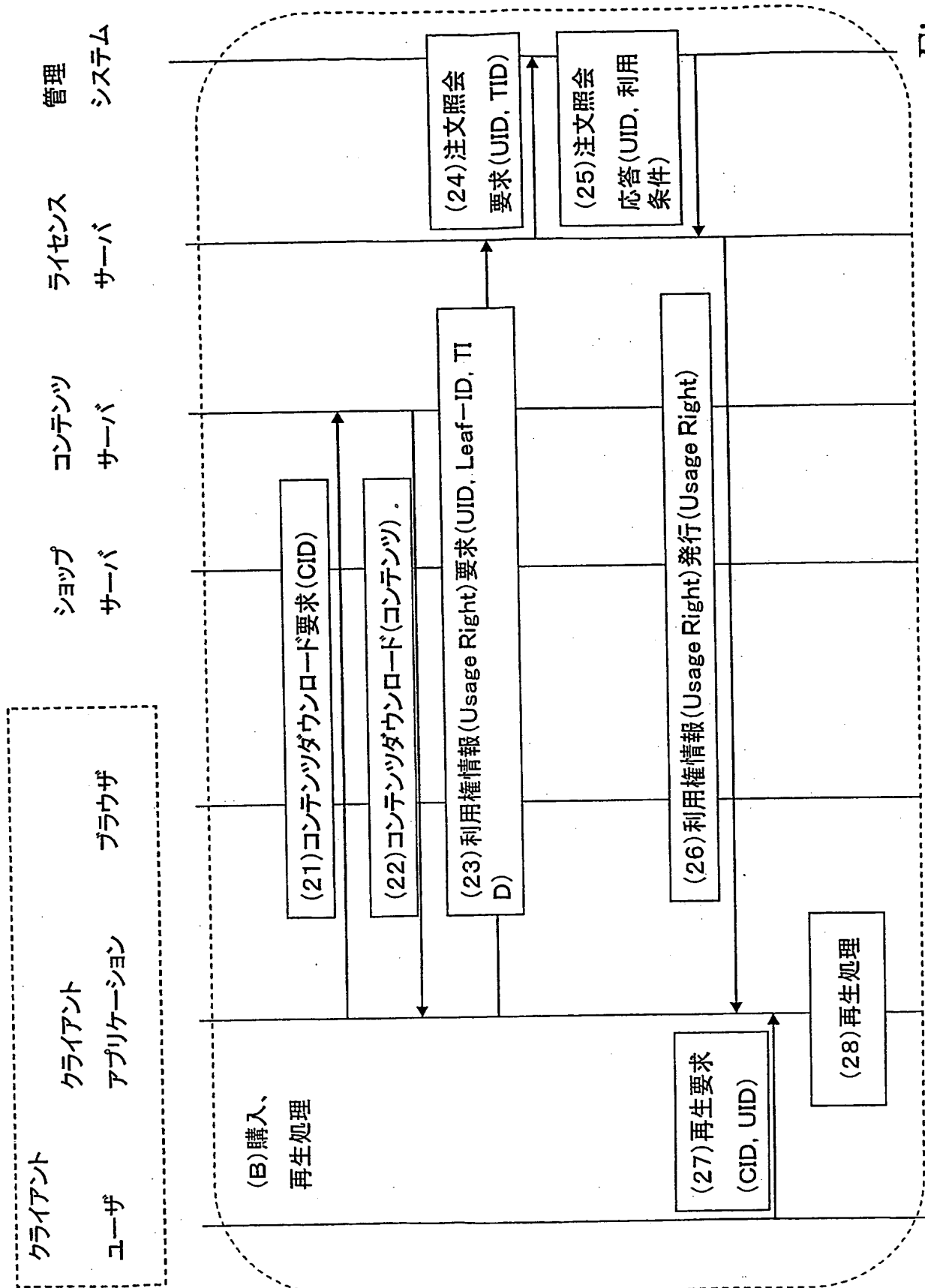


Fig. 18

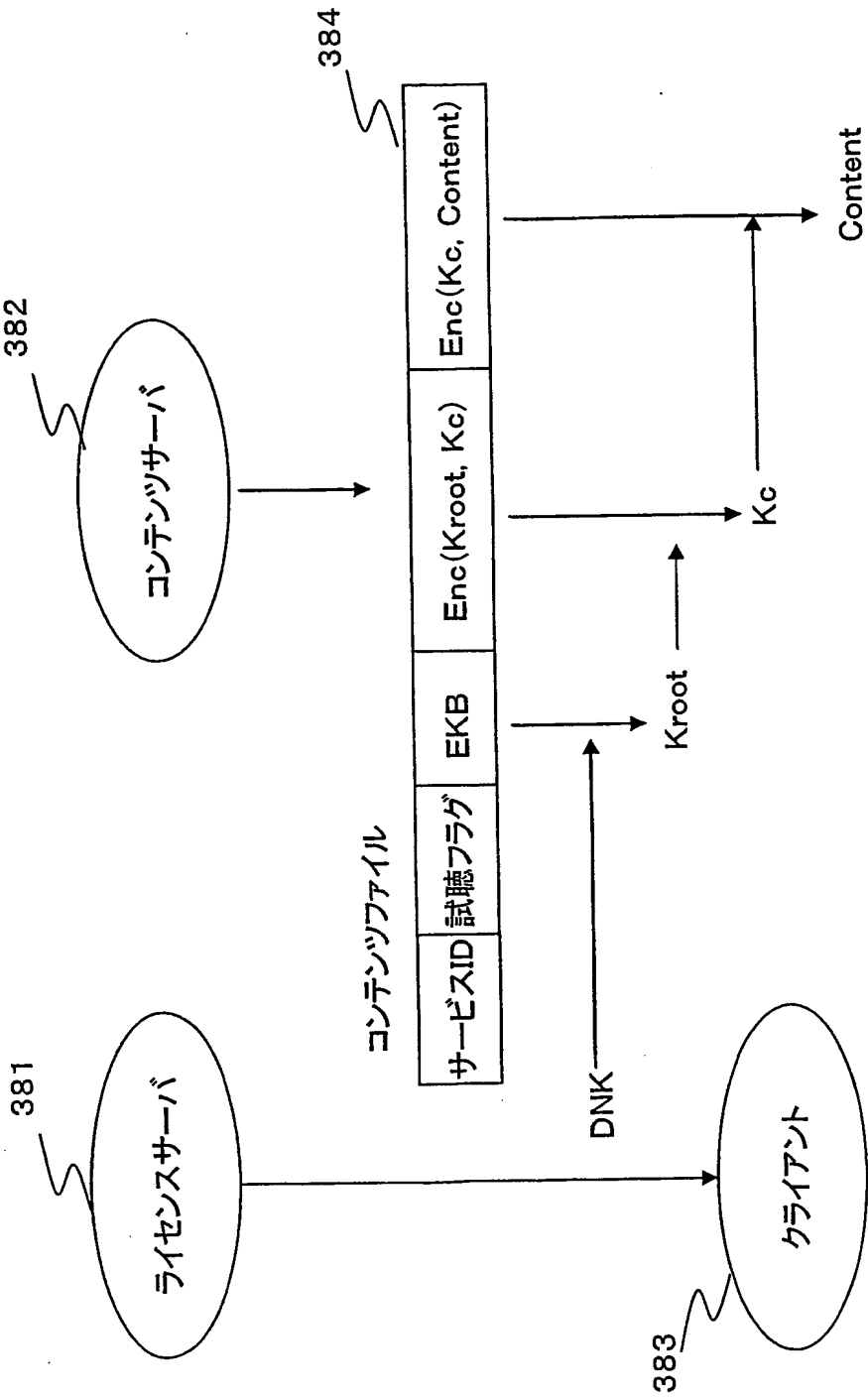
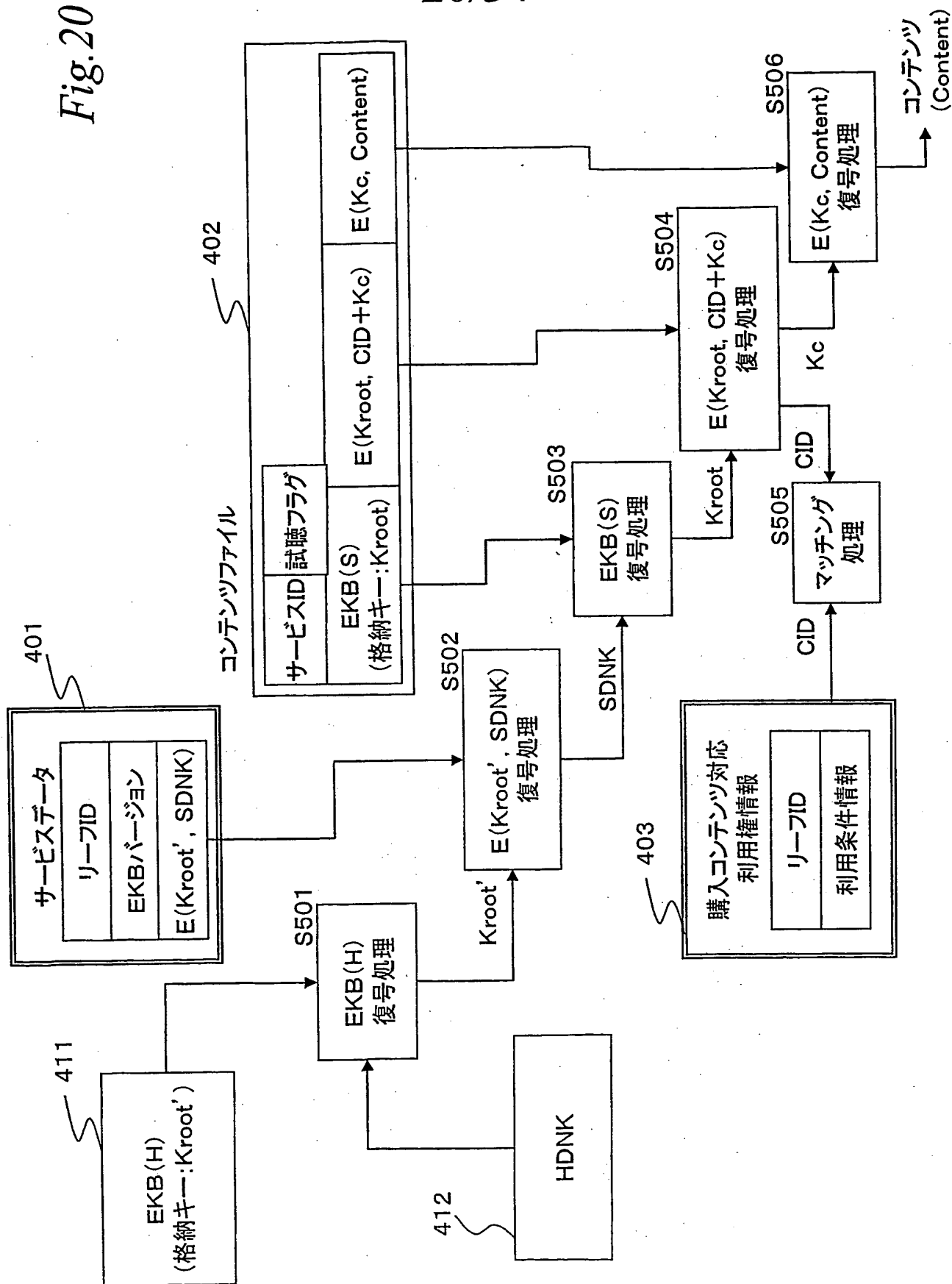


Fig.19

20/34

Fig. 20



21/34

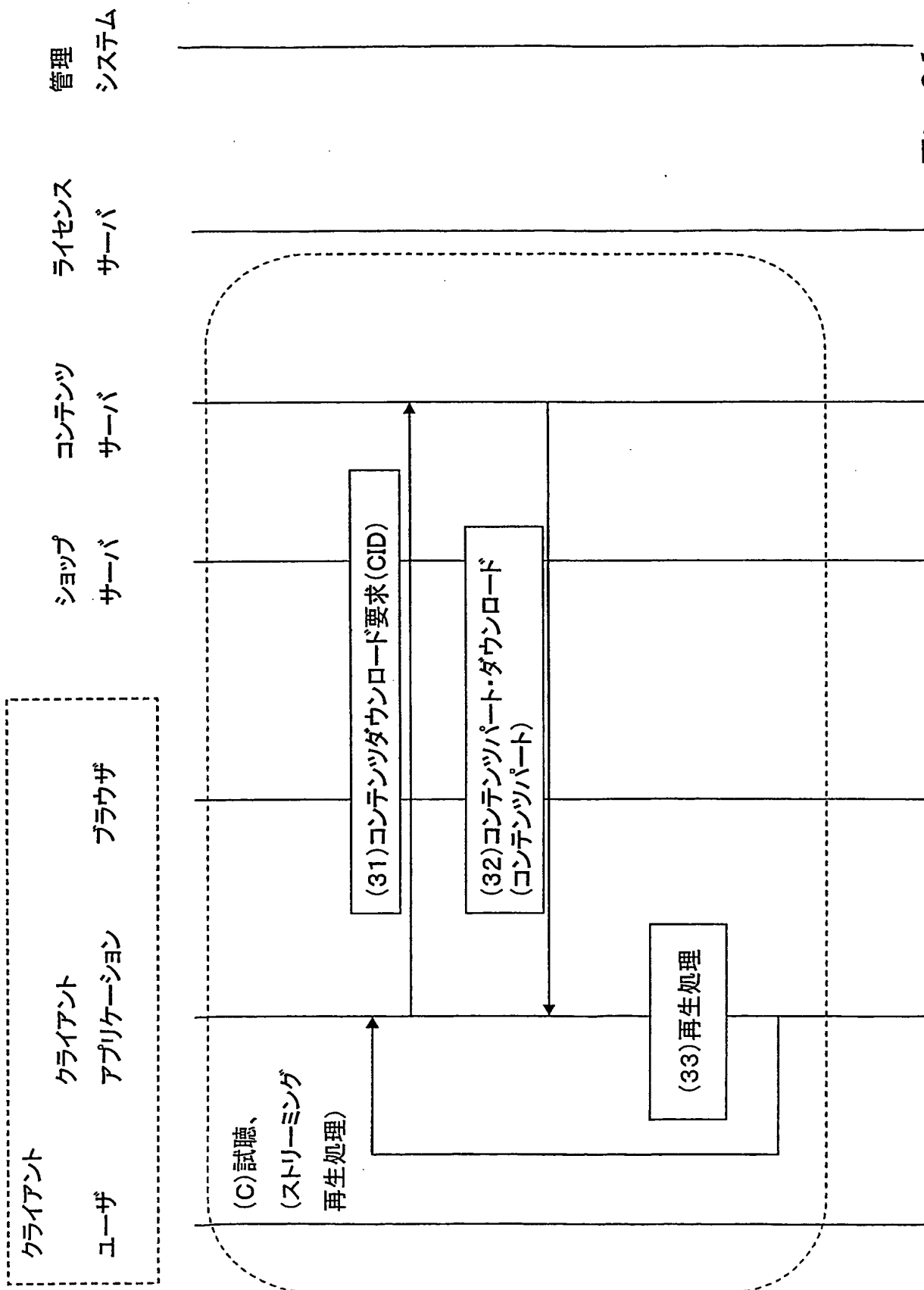


Fig.21

22/34

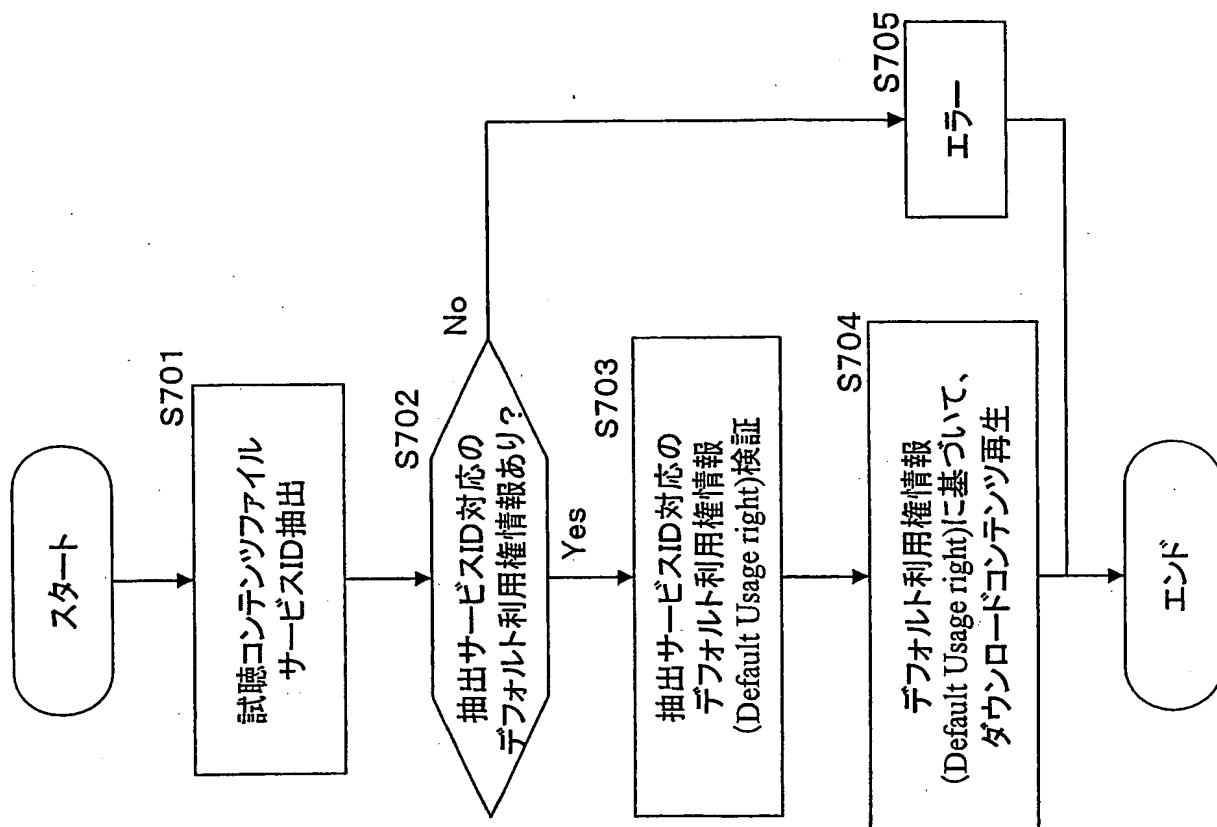


Fig. 22

23/34

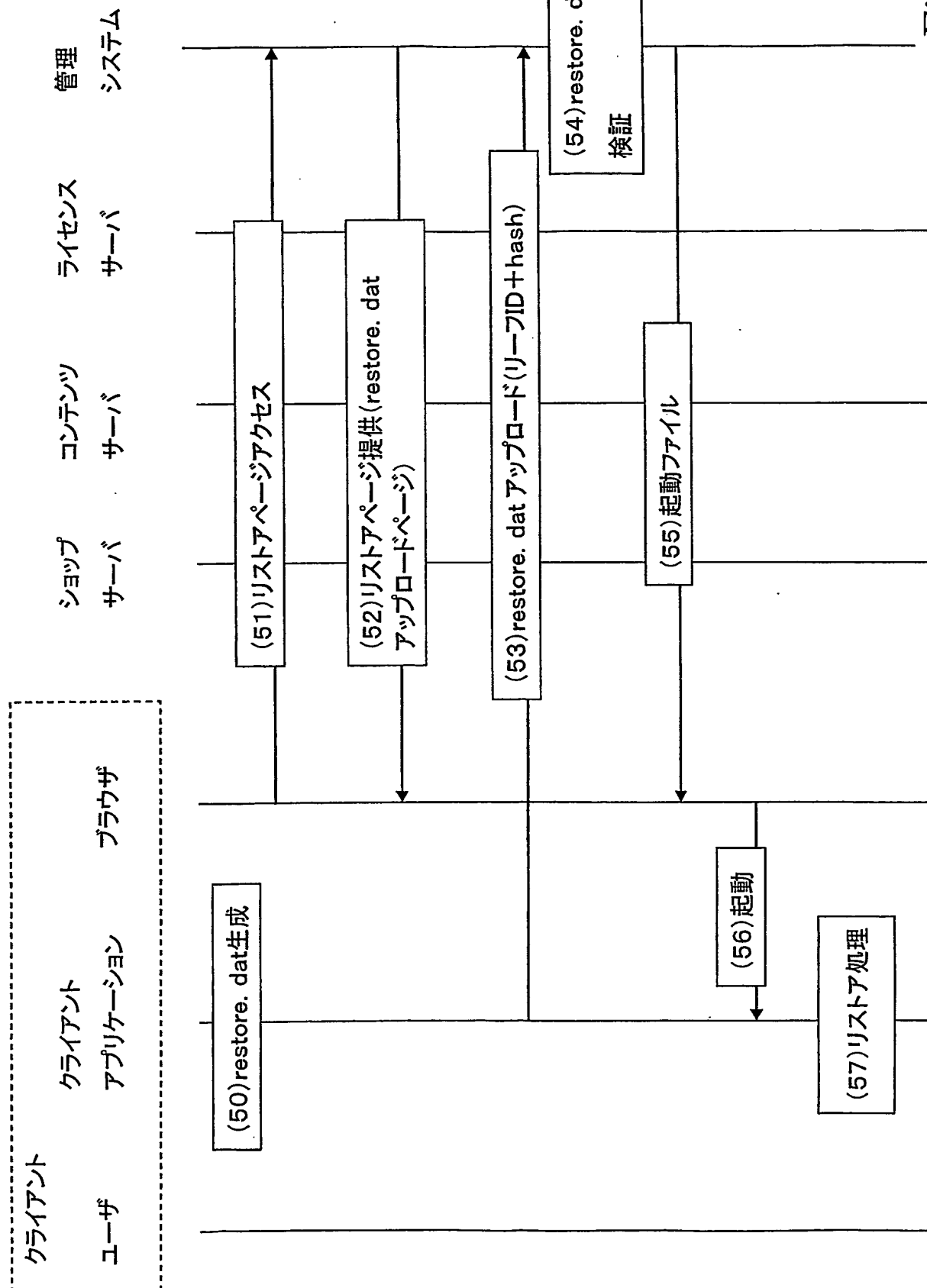


Fig.23

24/34

601

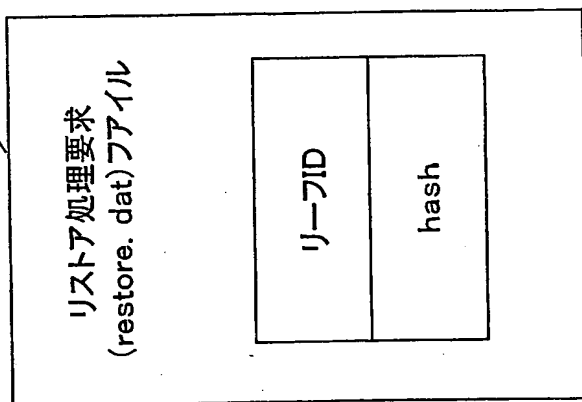
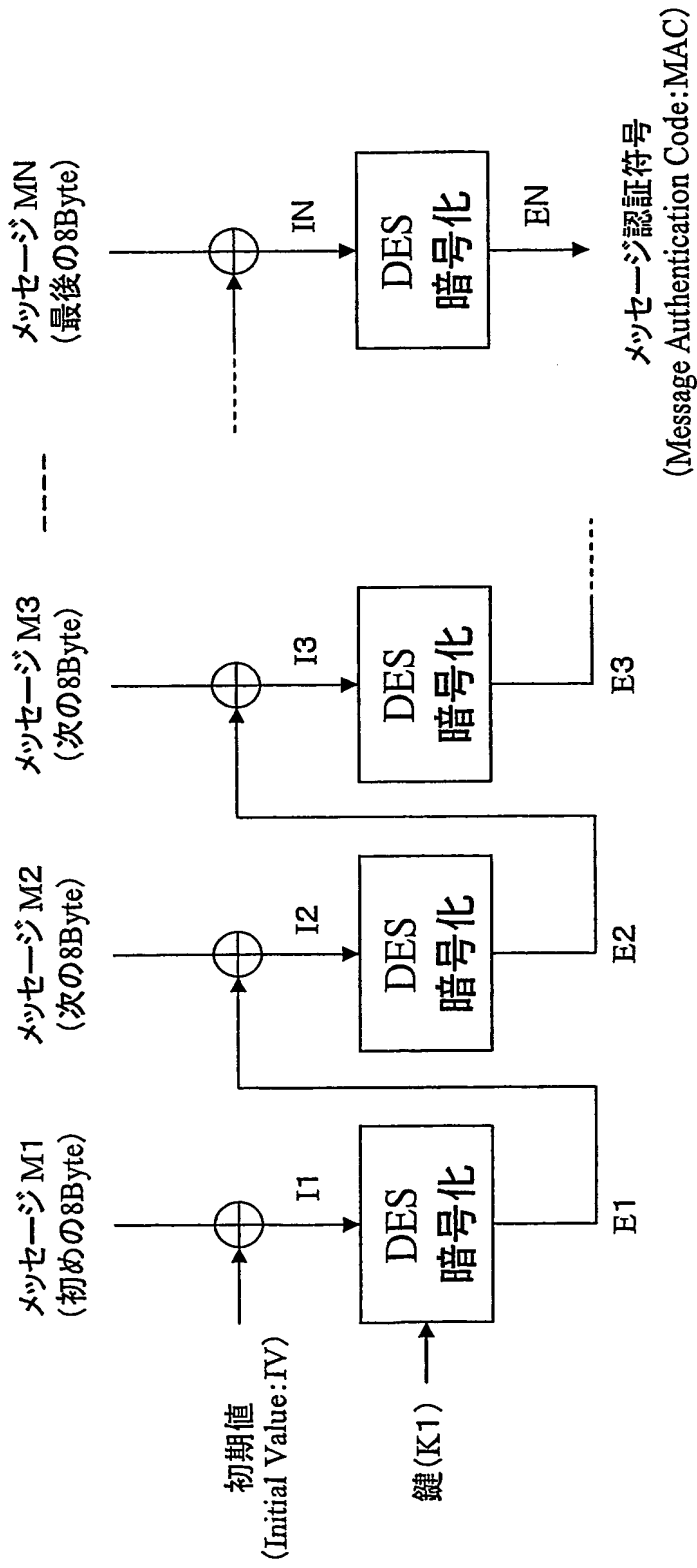


Fig. 24



⊕ : 排他的論理和処理(8バイト単位)

Fig.25

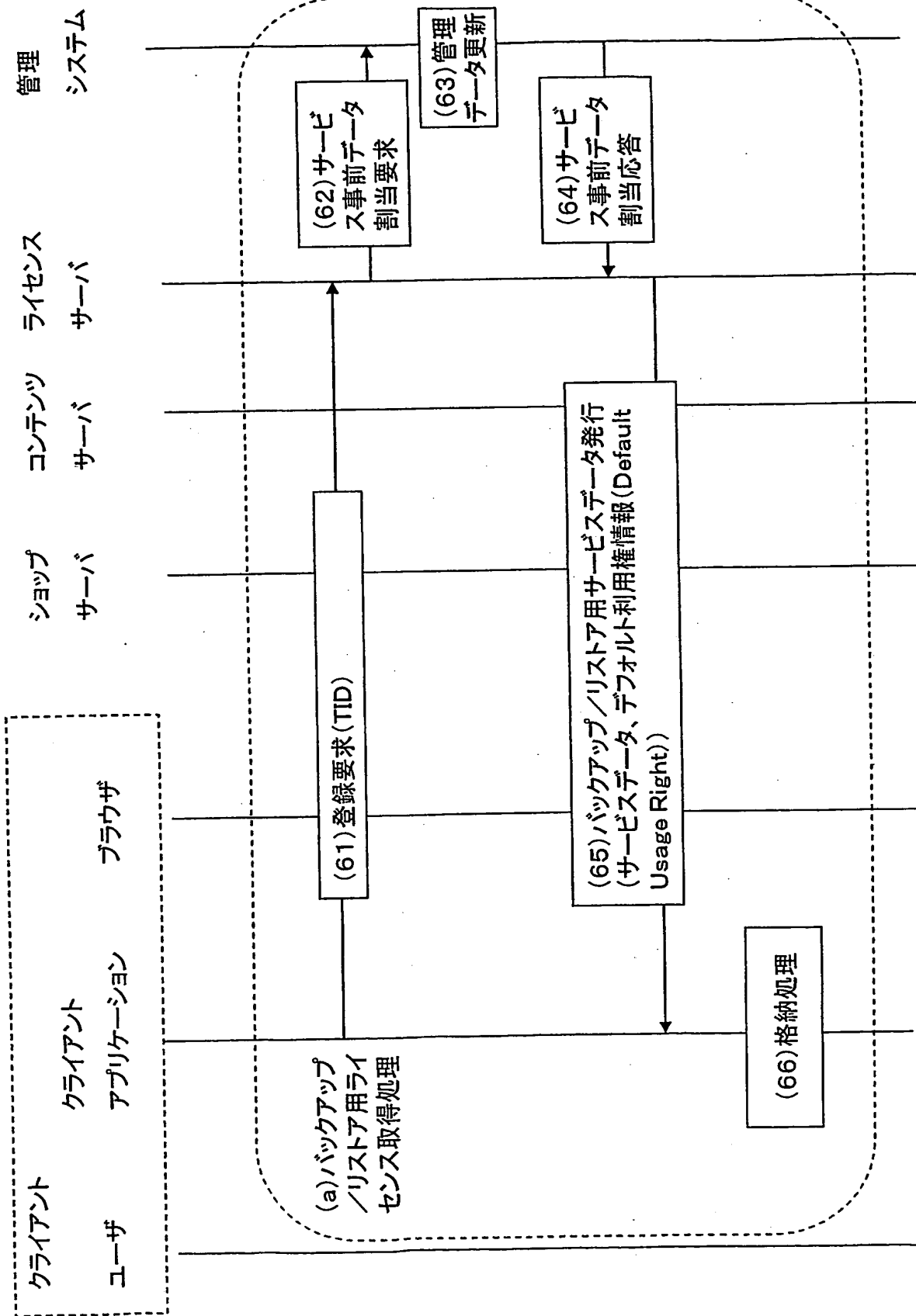


Fig. 26

27/34

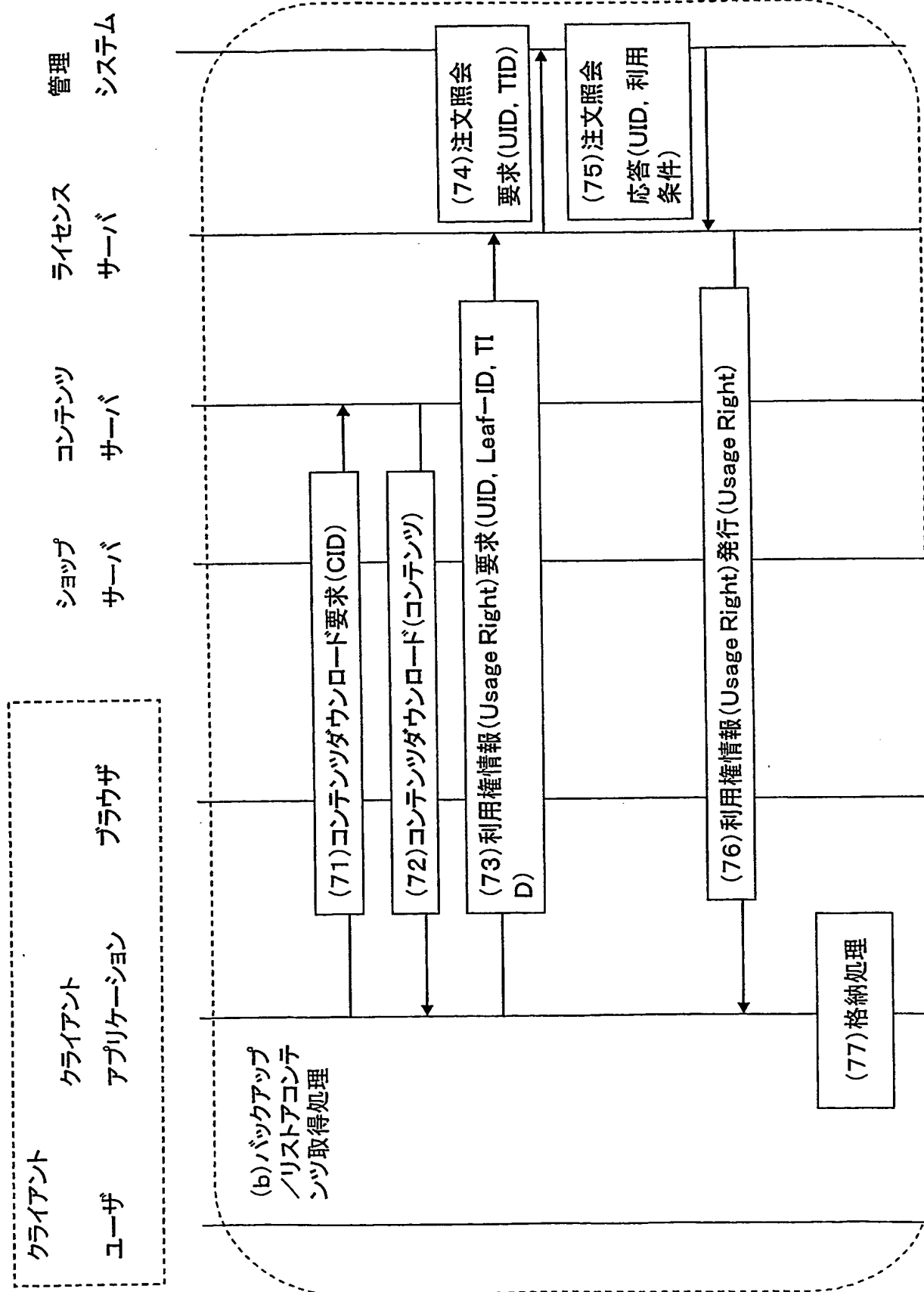
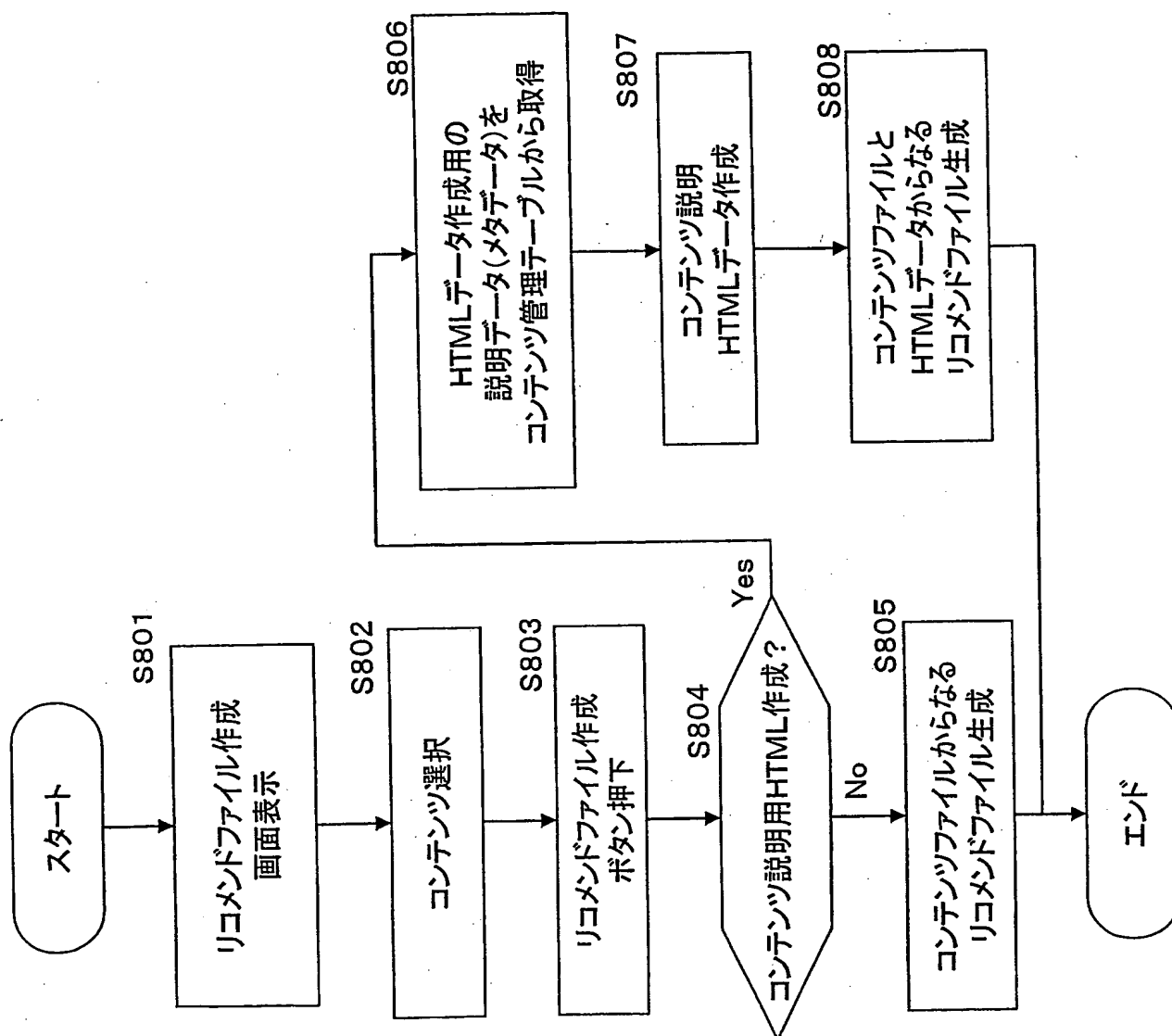


Fig.27

28/34

Fig. 28



29/34

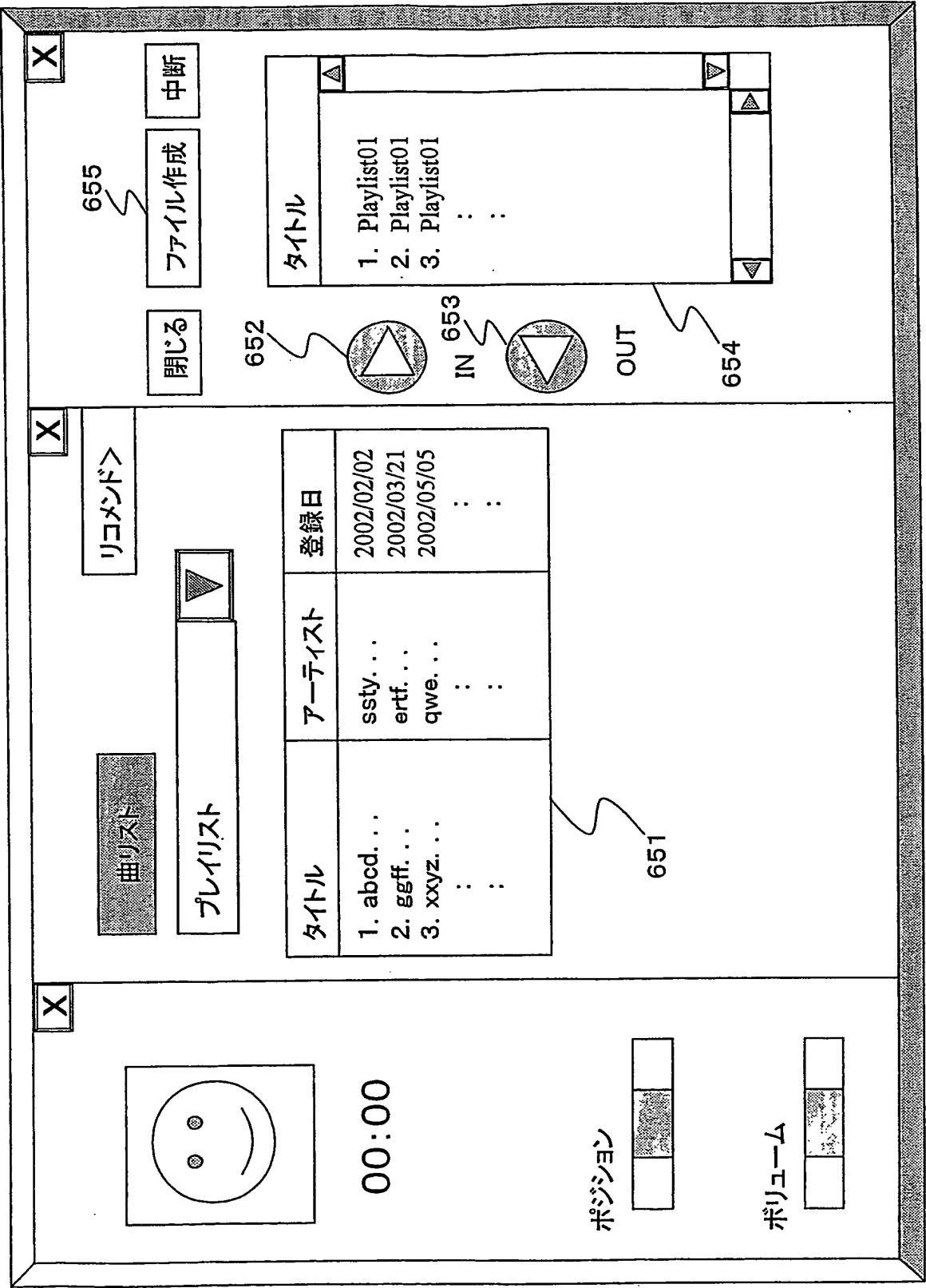


Fig. 29

30/34

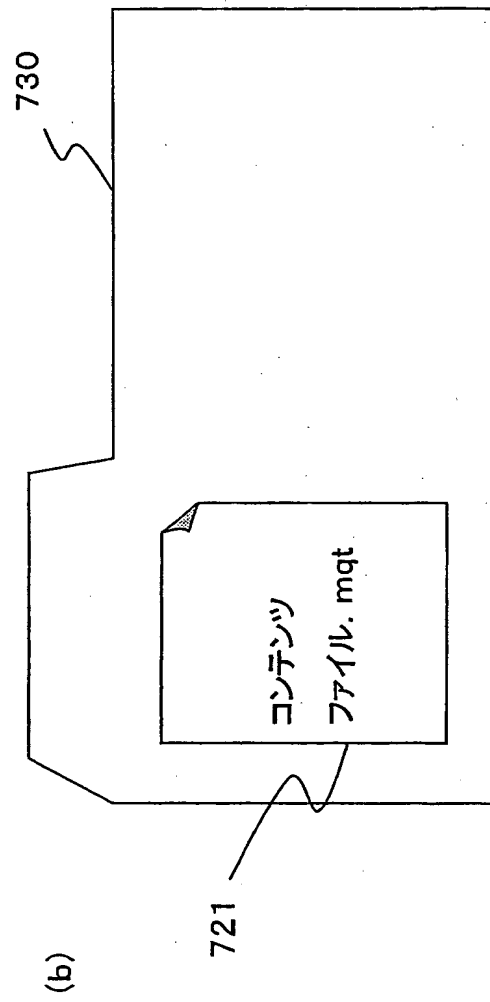
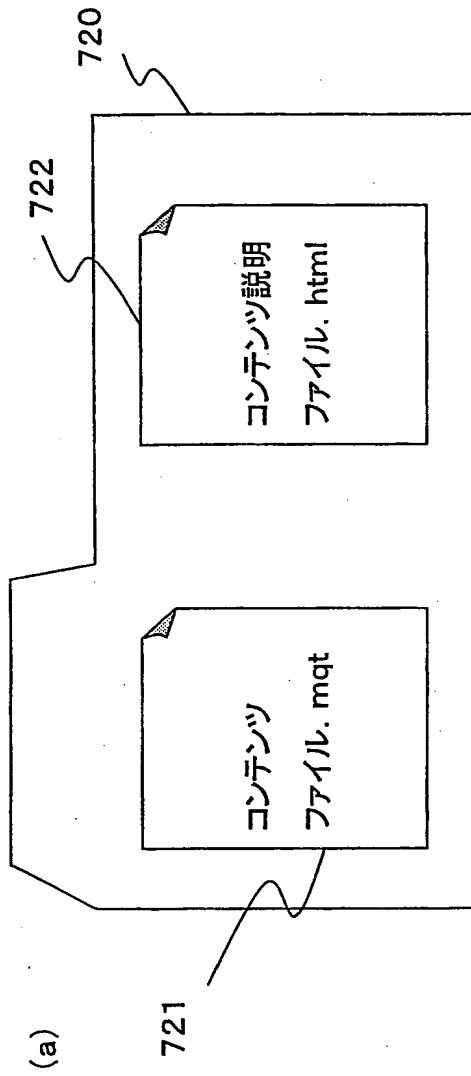


Fig.30

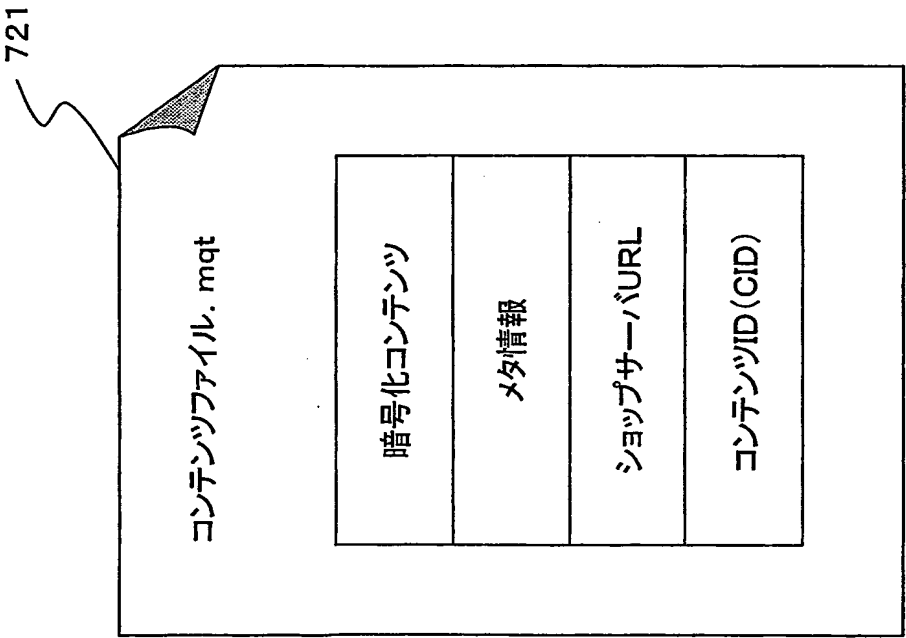


Fig.31

32/34

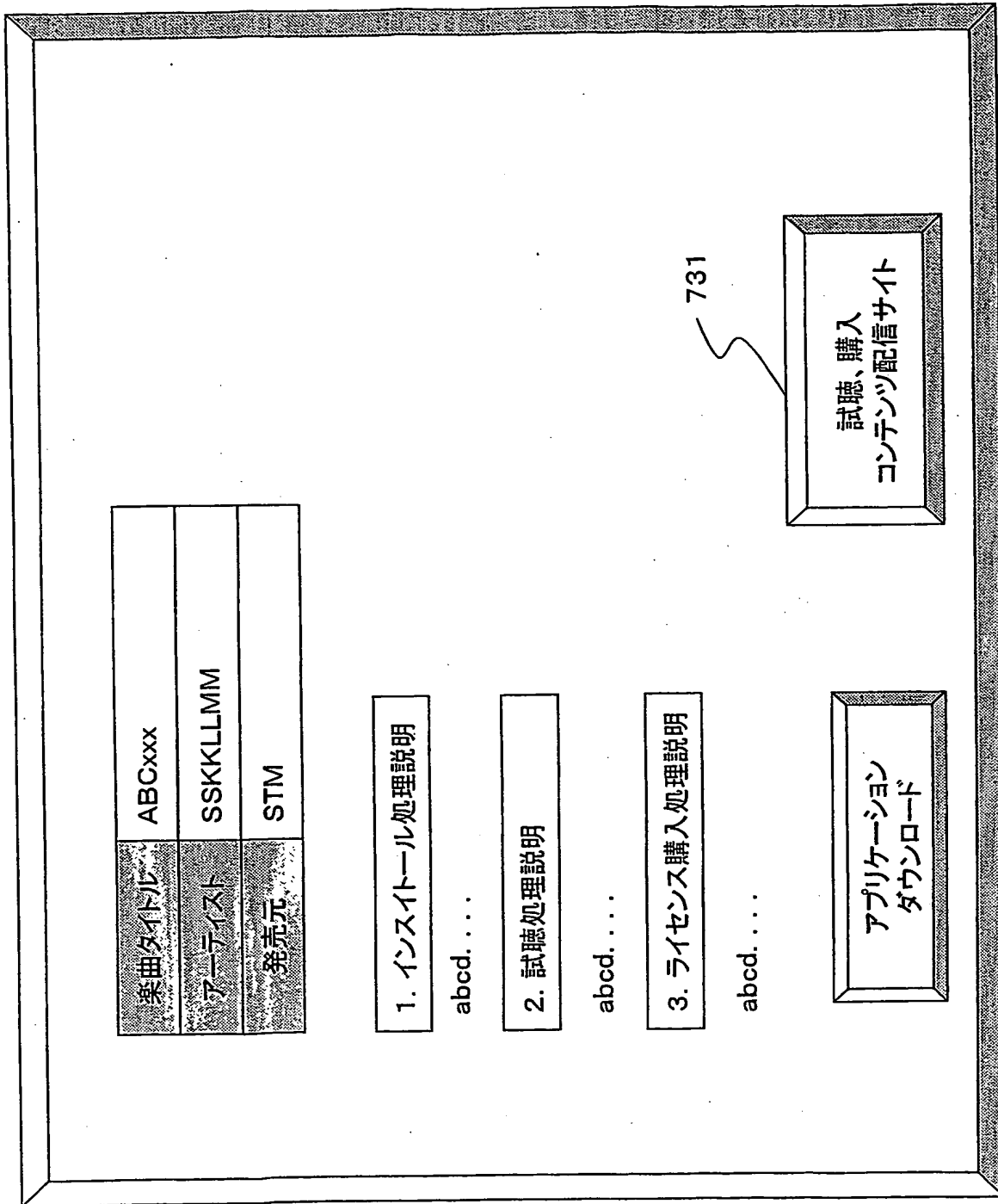


Fig.32

33/34

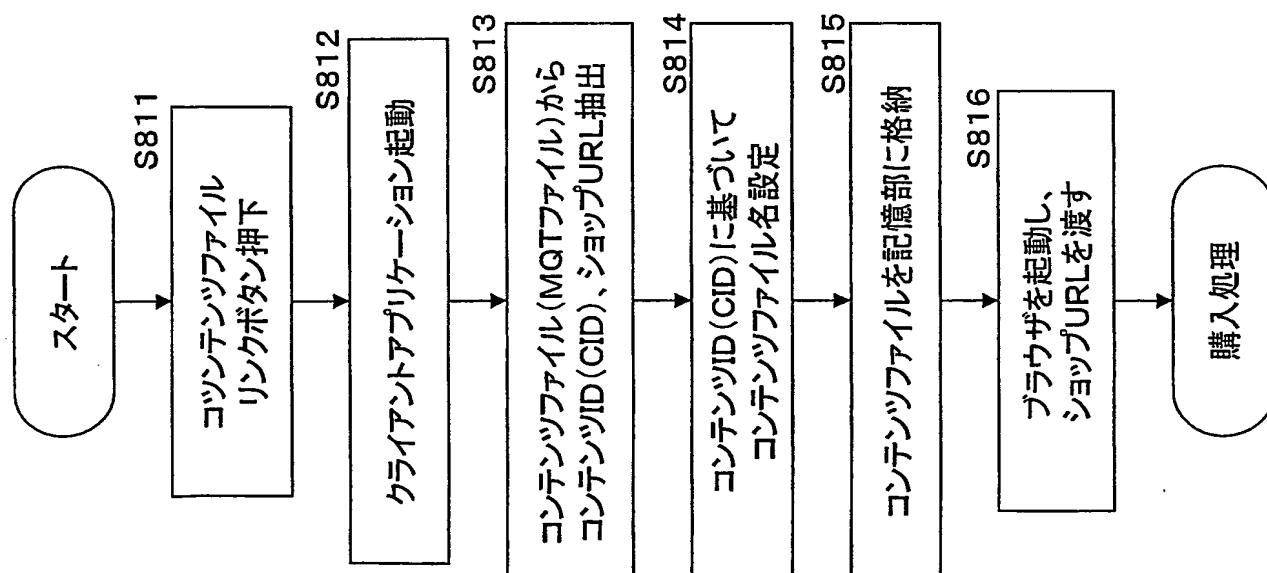


Fig.33

34/34

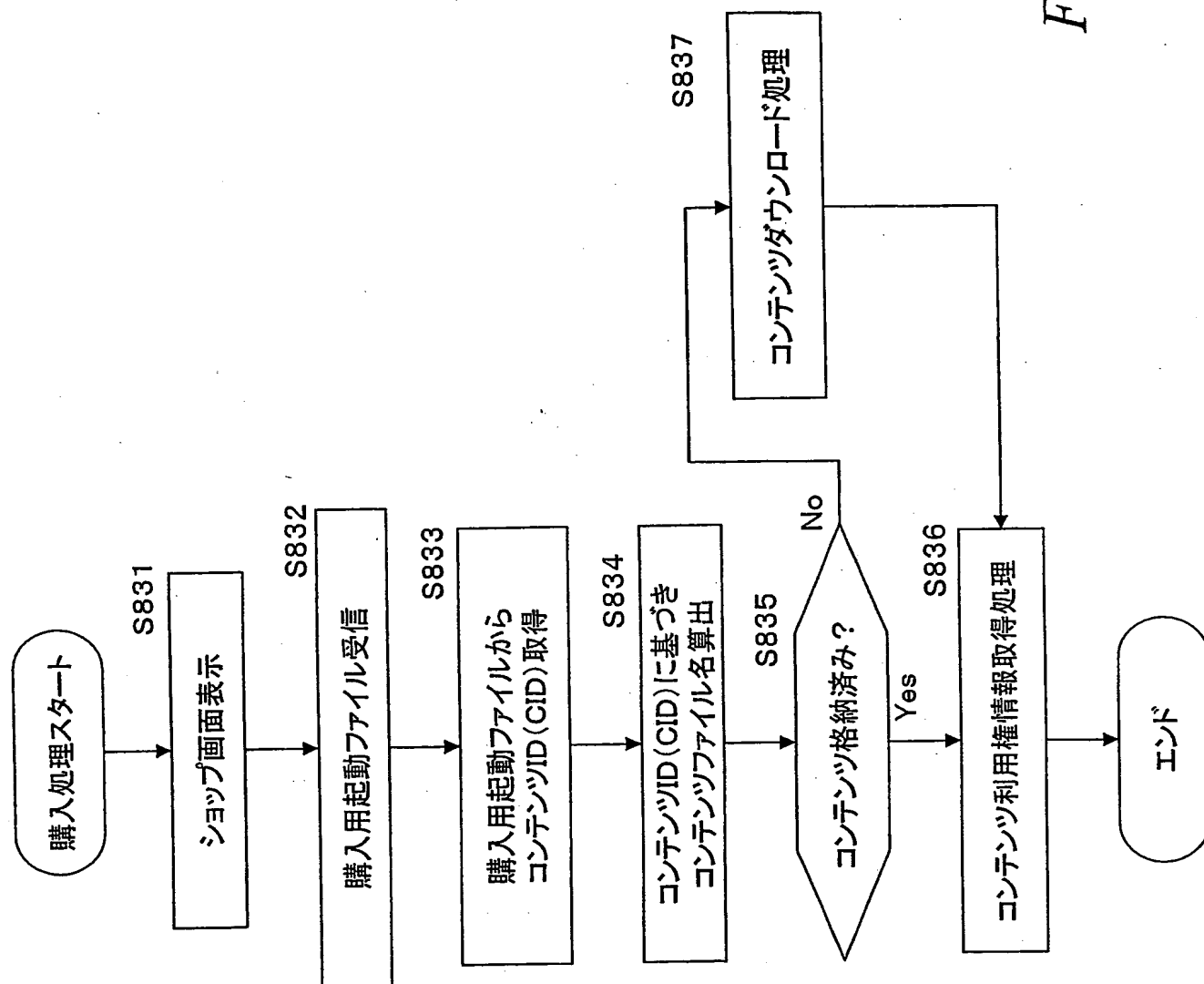


Fig. 34

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/08267

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F12/14, H04L9/08, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F12/14, H04L9/08, G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/44907 A1 (Microsoft Corp.), 21 June, 2001 (21.06.01),	1, 3-5, 11, 17, 19, 20
Y	All pages; all drawings & WO 01/44908 A1 & WO 01/46783 A2	2, 6-10, 12-16, 18
X	"Windows Media Rights Manager FAQ", [online], Microsoft Corporation, 2001, [retrieved on 2003-	1, 3-5, 11, 17, 19, 20
Y	09-04], Retrieved from the Internet: <URL: http:// web.archive.org/web/20010813233655/www.microsoft. com/japan/windows/windowsmedia/wm7/DRM/FAQ.asp? LNK=1>	2, 6-10, 12-16, 18

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
05 September, 2003 (05.09.03)

Date of mailing of the international search report
16 September, 2003 (16.09.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/08267

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Itaru HOSOMI, Masayuki NAKAE, Toshiharu ICHIYAMA, "Digital Joho Ryutsu Architecture MediaShell to sono Riyo-Kakin Seigyo", Information Processing Society of Japan Kenkyu Hokoku 98-EIP-2, Information Processing Society of Japan, 19 September, 1998 (19.09.98), Vol.98, No.85, pages 49 to 56	1,3-5,11, 17,19,20 2,6-10, 12-16,18
X	JP 2000-293439 A (Fujitsu Ltd.), 20 October, 2000 (20.10.00), All pages; all drawings (Family: none)	1,3-5,11, 17,19,20 2,6-10, 12-16,18
Y	JP 8-272746 A (Xerox Corp.), 18 October, 1996 (18.10.96), All pages; all drawings & US 5634012 A & EP 715243 A1	2,6-10, 12-16,18
Y	JP 7-221751 A (Nippon Telegraph And Telephone Corp.), 18 August, 1995 (18.08.95), All pages; all drawings (Family: none)	2,6-10, 12-16,18
Y	JP 9-297682 A (NEC Corp.), 18 November, 1997 (18.11.97), All pages; all drawings (Family: none)	2,6-10, 12-16,18
Y	JP 2002-133147 A (Fujitsu Ltd.), 10 May, 2002 (10.05.02), All pages; all drawings (Family: none)	2,6-10, 12-16,18

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, H04L9/08, G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, H04L9/08, G06F17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926 - 1996
 日本国公開実用新案公報 1971 - 2003
 日本国登録実用新案公報 1994 - 2003
 日本国実用新案登録公報 1996 - 2003

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO 01/44907 A1 (マイクロソフト コーポレイション) 2001.06.21, 全頁, 全図 & WO 01/44908 A1 & WO 01/46783 A2	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18

☒ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

05.09.03

国際調査報告の発送日

16.09.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号 100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

奥村 元宏

5N

3044

電話番号 03-3581-1101 内線 3585

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	"Windows Media Rights Manager FAQ", [online], Microsoft Corporation, 2001, [retrieved on 2003-09-04], Retrieved from the Internet: <URL: http://web.archive.org/we b/20010813233655/www.microsoft.com/japan/windows/windowsmedi a/wm7/DRM/FAQ.asp?LNK=1>	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18
X	細見 格, 中江 政行, 市山 俊治, " デジタル情報流通アーキテク チャMediaShellとその利用・課金制御", 情報処理学会研究報告 98-EIP-2, 社団法人情報処理学会, 1998. 09. 19, Vol. 98, No. 85, pp. 49-56	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18
X	JP 2000-293439 A (富士通株式会社) 2000. 10. 20, 全頁, 全図 (ファミリーなし)	1, 3-5, 11, 17, 19, 20
Y		2, 6-10, 12-16, 18
Y	JP 8-272746 A (ゼロックス コーポレーション) 1996. 10. 18, 全頁, 全図 & US 5634012 A & EP 715243 A1	2, 6-10, 12-16, 18
Y	JP 7-221751 A (日本電信電話株式会社) 1995. 08. 18, 全頁, 全図 (ファミリーなし)	2, 6-10, 12-16, 18
Y	JP 9-297682 A (日本電気株式会社) 1997. 11. 18, 全頁, 全図 (ファミリーなし)	2, 6-10, 12-16, 18
Y	JP 2002-133147 A (富士通株式会社) 2002. 05. 10, 全頁, 全図 (ファミリーなし)	2, 6-10, 12-16, 18

THIS PAGE BLANK (USPTO)